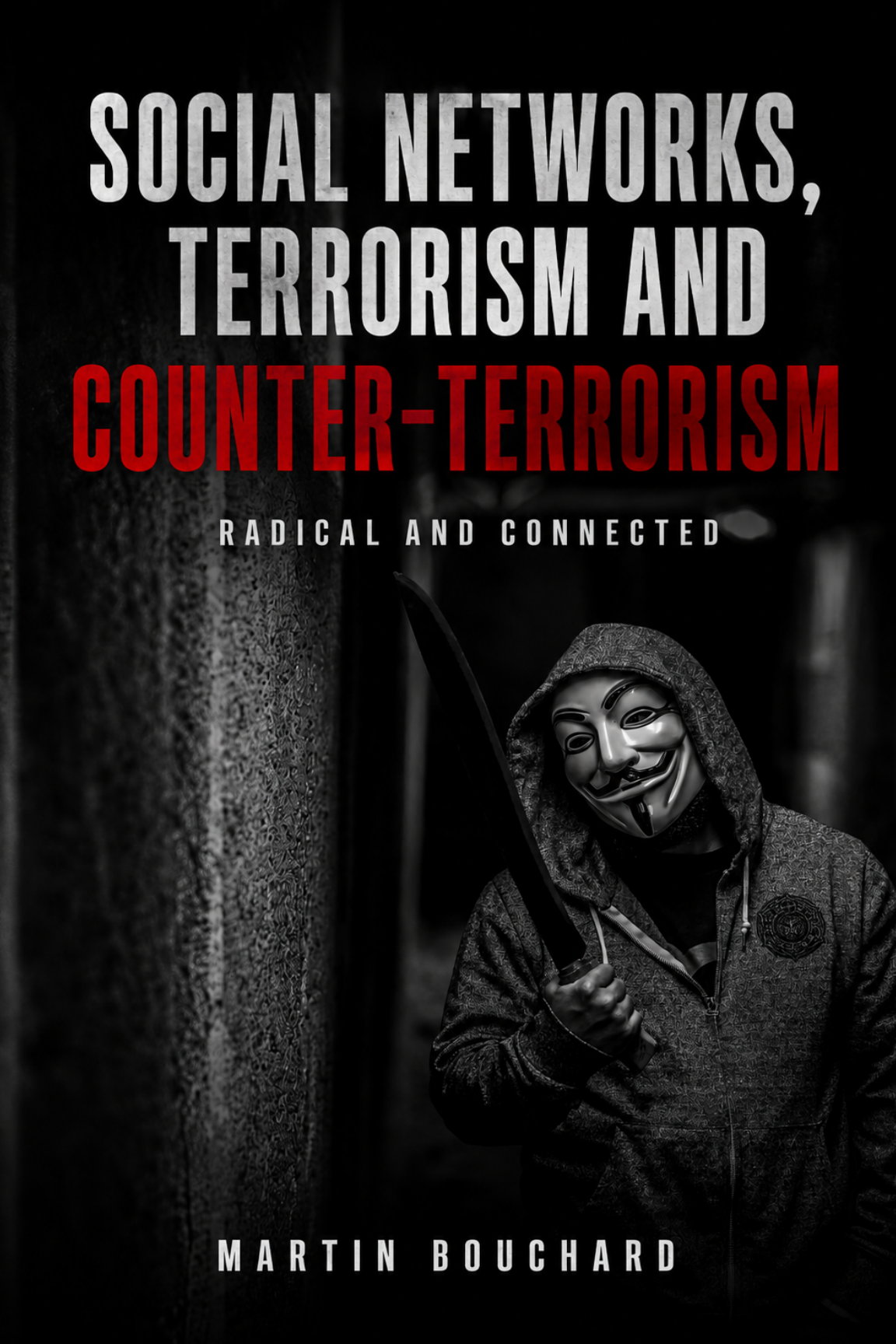
SOCIAL NETWORKS, TERRORISM AND COUNTER-TERRORISM

RADICAL AND CONNECTED



MARTIN BOUCHARD

Social Networks, Terrorism and Counter-terrorism

This book examines two key themes in terrorism studies, the radicalization process and counter-terrorism policies, through the lens of social networks.

The book aims to show that networks should be at the forefront not only when analyzing terrorists but also when assessing the responses to their actions. The volume makes a unique contribution by addressing two relatively new themes for terrorism studies. First, it puts social relations and cooperation issues at the forefront—an approach often identified as crucial to future breakthroughs in the field. Second, many contributions tackle the role of the Internet in the process of radicalization and in recruitment more generally, a highly debated topic in the field today. In addition, the book provides a valuable mix of review essays, critical essays, and original empirical studies. This balanced approach is also found in the topics covered by the authors, as well as their academic disciplines, which include sociology, computer science, geography, history, engineering and criminology as well as political science. Many of the true advances in terrorism studies depend on the successful collaboration of multi-disciplinary teams, each with a different set of methodological and conceptual tools. This volume reflects the newfound diversity in this field and is a true product of its time.

This book will be of much interest to students of terrorism studies, social networks, security studies, sociology, criminology and international relations in general.

Martin Bouchard is Associate Professor at the School of Criminology, Simon Fraser University, Canada. He is co-editor of *Illegal Markets and the Economics of Organised Crime* (Routledge 2010) and *World Wide Weed: Global Trends in Cannabis Cultivation and its Control* (Ashgate 2011) and editor of *Advances in Research on Illicit Networks* (Routledge 2015).

Contemporary Terrorism Studies

Understanding Terrorist Innovation
Technology, tactics and global trends
Adam Dolnik

The Strategy of Terrorism
How it works, why it fails
Peter Neumann and M.L.R. Smith

Female Terrorism and Militancy
Agency, utility, and organization
Edited by Cindy D. Ness

Women and Terrorism
Female activity in domestic and international terror groups
Margaret Gonzalez-Perez

The Psychology of Strategic Terrorism
Public and government responses to attack
Ben Sheppard

The De-radicalization of Jihadists
Transforming armed Islamist movements
Omar Ashour

Targeting Terrorist Financing
International cooperation and new regimes
Arabinda Acharya

Managing Terrorism and Insurgency
Regeneration, recruitment and attrition
Cameron I. Crouch

Religion and Political Violence
Sacred protest in the modern world
Jennifer L. Jefferis

International Terrorism Post-9/11
Comparative dynamics and responses
Edited by Asaf Siniver

Talking to Terrorists
Concessions and the renunciation of violence
Carolin Goerzig

Freedom and Terror
Reason and unreason in politics
Abraham Kaplan and Gabriel Weimann

Evaluating Counterterrorism Performance
A comparative study
Beatrice de Graaf

The EU and Counter-terrorism
Politics, polity and policies after 9/11
Javier Argomaniz

The Evolution of EU Counter-terrorism
European security policy after 9/11
Raphael Bossong

Conducting Terrorism Field Research
A guide
Edited by Adam Dolnik

US–UK Counter-terrorism after 9/11
A qualitative approach
Edgar B. Tembo

Transforming Violent Political Movements
Rebels today, what tomorrow?
Kevin Grisham

Radicalization in Western Europe
Integration, public discourse and loss of identity among Muslim communities
Carolin Goerzig and Khaled Al-Hashimi

Putting Terrorism in Context
Lessons from the Global Terrorism Database
Gary LaFree, Laura Dugan and Erin Miller

Al Qaeda's Global Crisis
The Islamic State, takfir, and the genocide of Muslims
V.G. Julie Rajan

Social Networks, Terrorism and Counter-terrorism
Radical and connected
Edited by Martin Bouchard

Social Networks, Terrorism and Counter-terrorism

Radical and connected

Edited by
Martin Bouchard

Routledge
Taylor & Francis Group
LONDON AND NEW YORK

First published 2015
by Routledge
2 Park Square, Milton Park, Abingdon, Oxon OX14 4RN

and by Routledge
711 Third Avenue, New York 10017

Routledge is an imprint of the Taylor and Francis Group, an informa business

© 2015 selection and editorial matter, Martin Bouchard; individual chapters, the contributors

The right of the editor to be identified as the author of the editorial matter, and of the authors for their individual chapters, has been asserted in accordance with sections 77 and 78 of the Copyright, Designs and Patents Act 1988.

All rights reserved. No part of this book may be reprinted or reproduced or utilized in any form or by any electronic, mechanical, or other means, now known or hereafter invented, including photocopying and recording, or in any information storage or retrieval system, without permission in writing from the publishers.

Trademark notice: Product or corporate names may be trademarks or registered trademarks, and are used only for identification and explanation without intent to infringe.

British Library Cataloguing-in-Publication Data
A catalogue record for this book is available from the British Library

Library of Congress Cataloging-in-Publication Data
Social networks, terrorism and counter-terrorism : radical and connected / edited by Martin Bouchard.
pages cm. – (Contemporary terrorism studies)
Includes bibliographical references and index.
1. Terrorism. 2. Internet and terrorism. 3. Terrorists–Social networks. 4. Terrorism–Prevention. I. Bouchard, Martin, 1981- editor.
HV6431.S6433 2015
363.325–dc23 2014048211

ISBN: 978-1-138-82856-8 (hbk)
ISBN: 978-1-315-73829-1 (ebk)

Typeset in Times New Roman
by Wearset Ltd, Boldon, Tyne and Wear

Contents

List of figures ix
List of tables x
Notes on contributors xi
Foreword xvi
DANIEL HIEBERT AND LORNE L. DAWSON

1 Radical and connected: an introduction 1
MARTIN BOUCHARD AND PHILIPPA LEVEY

PART I
Terrorism and radicalization: history, networks and the Internet 9

2 The roots of terrorism in the Middle East 11
ANDRÉ GEROLYMATOS

3 The gray cygnet problem in terrorism research 34
LAURA HUEY, JOSEPH VARANESE AND RYAN BROLL

4 Researching terrorism and counter-terrorism through a network lens 48
MARTIN BOUCHARD AND REBECCA NASH

5 Travel broadens the network: turning points in the network trajectory of an American jihadi 61
REBECCA NASH AND MARTIN BOUCHARD

6 A radical sociability: in defense of an online/offline multidimensional approach to radicalization 82
BENJAMIN DUCOL

7 Terrorist and extremist organizations' use of the Internet for recruitment 105
GARTH DAVIES, MARTIN BOUCHARD, EDITH WU, KILA JOFFRES AND RICHARD FRANK

8 Exploring the behavioral and attitudinal correlates of civilian cyberattacks 128
THOMAS J. HOLT, MAX KILGER, LICHUN CHIANG AND CHU-SING YANG

PART II
Counter-terrorism: prospects, pitfalls, policies 153

9 Security networks and counter-terrorism: a reflection on the limits of adversarial isomorphism 155
BENOÎT DUPONT

10 The promise and perils of integrated models of public safety in Canada 175
VERONICA M. KITCHEN AND ADAM MOLNAR

11 A systematic approach to developing a computational framework for counter-terrorism and public safety 196
ANDREW J. PARK AND HERBERT H. TSANG

12 Radical and connected: concluding thoughts and future research 218
MARTIN BOUCHARD AND EVAN THOMAS

Index 231

Figures

5.1 Full personal network of Hammami from his pre-jihad days to Al-Shabaab 69
5.2 Hammami's pre-jihad network in Daphne, USA, and Toronto, Canada 73
5.3 Hammami's network in Alexandria, Egypt, and Mogadishu, Somalia 74
5.4 Hammami's Somalia network—three cities combined 75
5.5 Hammami's network density by time period and location 76
5.6 The proportion of ties in Hammami's network by time period and location 77
6.1 Situational action theory: simplified framework 92
6.2 Online and offlines life-spheres and the production of a sociability 95
6.3 The emergence of a radical sociability 96
7.1 Recruitment and extremism scales 121
11.1 Classification of crowds 200
11.2 The 3D visualization of a crowd in the GENIUS system 201
11.3 Initial setup and plots of a typical run in Scenarios A and B 204
11.4 The layout of the simulation of the Boston Marathon bombings 206
11.5 Simulations of the Boston Marathon bombings 207
11.6 Simulations of the Westgate Shopping Mall attack 208
11.7 Initial setup and plots of a typical run in Scenario C 210
11.8 The current setup of GENIUS 214

Tables

5.1	Top 10 brokers in Hammami's full network	71
7.1	The website extremism scale	116
7.2	The website recruitment scale	116
7.3	The recruitment checklist	118
7.4	Keywords	120
7.5	Typology of recruitment websites	123
7.6	Typology of recruitment websites—examples	124
7.7	General characteristics of sampled websites	125
8.1	Sample descriptives	134
8.2	Binary logistic regression models for defacing government servers	138
8.3	Binary logistic regression models for searching government servers	142
8.4	Binary logistic regression models for compromising military servers	144
9.1	Three organizational morphologies	159

Contributors

Martin Bouchard is an associate professor of Criminology at Simon Fraser University, Canada, and director of the International Cybercrime Research Centre (ICCRC). His work focuses on the role of social networks in various criminal career outcomes, including those of violent radicals. His work has appeared in numerous journals, including *Journal of Quantitative Criminology*, *Journal of Research in Crime and Delinquency*, *Justice Quarterly* and *Social Networks*. He has co-edited three books prior to the current volume, including *Advances in Research on Illicit Networks* in 2015 (Routledge). He won the SFU 2013 Dean of Graduate Studies award for excellence in supervision.

Ryan Broll is an assistant professor in the department of Sociology and Legal Studies at University of Guelph. His research areas include cyberpolicing, cyberbullying and criminal investigation.

Lichun Chiang is an associate professor in the Department of Political Science in National Cheng Kung University in Taiwan. Her research interests are e-government and information ethics.

Garth Davies is an associate professor of Criminology at Simon Fraser University. His primary field of study is advanced statistical analysis. He has been writing and teaching about terrorism for over 15 years. He is currently collaborating on the development of the Terrorism and Extremism Network Extractor (TENE), a web-crawler designed to investigate extremist activities on the Internet.

Lorne L. Dawson is the chair of the Department of Sociology and Legal Studies at the University of Waterloo (since 2011). He is a professor in the Department of Sociology and Legal Studies and the Department of Religious Studies, which he chaired as well (2000–2006). Most of his research is in the sociology of religion, particularly the study of new religious movements, and he is perhaps best known for his book *Comprehending Cults: The Sociology of New Religious Movements* (2nd edn, Oxford University Press, 2006). He is also the co-director of the Canadian Network for Research on Terrorism, Security and Society.

Benjamin Ducol is a PhD candidate in Political Science at the Université Laval, Québec and a research affiliate with the Canada Research Chair on Conflicts and Terrorism. His research focus is in the field of terrorism studies with a specialization on issues surrounding the role of the Internet on terrorism and radicalization processes. His work appeared in multiple peer-reviewed scientific journals, including *Terrorism and Political Violence*, *Media War and Conflict* and *Civil Wars*.

Benoît Dupont is a Canada Research Chair in Security, Identity and Technology at the Université de Montréal. He is also the scientific director at SERENE-RISC Smart Cybersecurity Network, one of Canada's Networks of Centres of Excellence, and a member of the expert panel on policing models for the Canadian Council of Academies. His work has focused on cybercrime, security governance and public–private partnerships in the provision of security.

Richard Frank is an assistant professor at the School of Criminology at Simon Fraser University. He has 35 peer-reviewed publications, with recent publications at top-level data mining outlets such as in Knowledge Discovery in Databases, and security conferences such as Intelligence and Security Informatics. He developed the CENE software (predecessor to TENE) that has been used at the International CyberCrime Research Center (ICCRC) to study child exploitation websites. He is the associate director of the ICCRC.

André Gerolymatos is a professor of History, an associate professor in the School of Criminology, and director of the SNF Centre for Hellenic Studies at Simon Fraser University. He has published several books including the *International Civil War: Greece 1943–1949* (2015) and *Castles Made of Sand: A Century of Anglo-American Espionage and Intervention in the Middle East* (2010). A member of the Canadian Advisory Council on National Security from 2010 to 2012, he is a specialist in national security, military, diplomatic and intelligence history, regularly contributing numerous articles for online and print media, and is often interviewed on topics concerning national security.

Daniel Hiebert is a professor at the University of British Columbia. Among his main research areas are international migration, the consequences of immigration in Canadian cities, and the integration of newcomers in the labor and housing markets of cities. His work is highly integrated with public policy, as he participates in advisory roles at the local and national level in Canada and partakes in regular interactions with government agencies in several other countries. He is working with a large network of scholars on the issue of national security and its relationship with human rights.

Thomas J. Holt is an associate professor in the School of Criminal Justice at Michigan State University specializing in cybercrime, policing and policy. He received his PhD in Criminology and Criminal Justice from the University of

Missouri–Saint Louis in 2005. He has published extensively on cybercrime and cyberterror in outlets such as *Crime and Delinquency*, *Journal of Criminal Justice, Terrorism and Political Violence* and *Deviant Behavior*. He is a member of the International CyberCrime Research Center (ICCRC) and a founding member of the Spartan Devils Chapter of the International Honeynet Project.

Laura Huey is an associate professor in the Department of Sociology at the University of Western Ontario. She holds a PhD in Sociology from the University of British Columbia. She is the author of several articles on issues related to victimization, policing, cybercrime and surveillance. Her research has appeared in *Society and Mental Health*, *Journal of Interpersonal Violence* and other international journals. She has authored two books on the provision of security for homeless victims of crime and is co-editor of a collection on alternative forms of policing. Her research interests are policing (frontline and criminal investigation); victimization of the homeless; cybercrime; cyber-policing; and online radicalization.

Kila Joffres is a doctoral student in Criminology at Simon Fraser University. Her research interests include examining the use of network analysis in policing, particularly for online child pornography and extremist networks. Her work on these issues appeared in a recent volume of *Crime Prevention Studies*.

Max Kilger received his doctorate from Stanford University in Social Psychology in 1993. He is a senior lecturer at the University of Texas at San Antonio with a joint appointment in the Cyber Security Department. Max is a founding member of the Honeynet Project information security research group and is their chief membership officer. He is also the project's chief profiler and contributes in the areas of statistical and data analysis.

Veronica M. Kitchen is an associate professor of Political Science at the University of Waterloo and in the Balsillie School of International Affairs. She researches the global governance of domestic security, focusing on urban security and counter-terrorism, security bureaucracies, the ethics of security, North American security governance, and mega-event security.

Philippa Levey is a graduate student in the School of Criminology at Simon Fraser University, with a focus on terrorism, cyberterrorism and social networks. She is a research assistant for the International CyberCrime Research Center (ICCRC) at Simon Fraser University.

Adam Molnar is a lecturer in Criminology at Deakin University, Australia. He specializes in practices of policing and national security as they relate to technology, surveillance and issues of privacy. He is researching the surveillance and privacy implications of the domestic application of unmanned aerial vehicles in Australia and Canada and continues to research and publish on policing, technology, and privacy, as well as on inter-organizational initiatives in policing and national security.

Rebecca Nash is an assistant professor of Criminal Justice at California State University in Long Beach. Her research interests are concentrated in white-collar crime and counter-terrorism within the policing paradigm. Her research in these areas has an interdisciplinary focus drawing from the fields of criminology, sociology, and economics—especially through network theory and diffusion theory—in understanding illicit networks. Her teaching focus is in quantitative research methods using a variety of methodological applications, including social network analysis, GIS crime mapping and statistical analysis. Recent research includes mapping an illicit fraud network to better understand how financial decision-making is embedded in social relations.

Andrew J. Park is an assistant professor of Computing Science at Thompson Rivers University, Kamloops, British Columbia, and a senior research fellow at the Institute for Canadian Urban Research Studies. His research areas include counter-terrorism, crowd simulation, virtual environment, agent-based modeling and simulation, information visualization, computational criminology, social network analysis, and human–computer interaction.

Evan Thomas is a graduate student in the School of Criminology at Simon Fraser University. With a focus on social networks, cyberterrorism, and terrorism, he is a research assistant for the International CyberCrime Research Center (ICCRC) at Simon Fraser University.

Herbert H. Tsang is an associate professor of Computing Science and Mathematics at Trinity Western University, Langley, British Columbia, and an adjunct professor at Simon Fraser University, Burnaby, British Columbia. His research areas include bioinformatics, computational modeling, signal processing and scientific visualization. He is a senior member of IEEE and a professional engineer in the province of British Columbia. He previously worked at MacDonald Dettwiler and Associates Ltd as a member of the scientific and engineering staff.

Joseph Varanese is the CPRN social media coordinator and the individual responsible for keeping members up to date on the latest CPRN news and events. He is also a Master's student at Western and a member of TSAS. His work explores issues related to security intelligence, domestic radicalization and the funding of terrorist groups.

Edith Wu is a graduate student in the School of Criminology at Simon Fraser University. With a primary focus in political violence, she has published work in perspectives on terrorism regarding Al-Qaeda and its leadership.

Chu-Sing Yang is a professor in the Department of Electrical Engineering/ Graduate Institute of Computer and Communication Engineering, NCKU, and Director of TWISC@NCKU. He has been awarded First Prize in Open-sourced Hardware and Embedded System Competitions, "A Traffic Management System based on NetFPGA in OpenFlow Virtualized Network environment," 2012; as well as the Golden prize in the International Salon of

Inventions and the Technologies, "Brightness Adjustment Metheod and System with Photographic Device." His specialties are internet technology, network monitoring and management; software defined networking, SDN—OpenFlow; pervasive computing, smart home, RFID, UPnP, OSGi; surveillance systems, image processing, wireless networks, wireless sensor networks; and embedded systems, NetFPGA.

Foreword

Daniel Hiebert and Lorne L. Dawson

This book was born out of an event where international researchers and policy-makers came together in Ottawa, Canada, to discuss some of the most pressing issues in the area of terrorism and counter-terrorism. The event was organized by Martin Bouchard and the team working at the Canadian Network for the Study of Terrorism, Security, and Society (TSAS). TSAS was created in 2012 to foster interdisciplinary research on terrorist radicalization, the coordinated interaction of academic researchers with government officials, and the cultivation of a new generation of young scholars interested in terrorism, security, and the impact of both on society. Prior to the formation of TSAS, there was no other organization of its type in Canada. Policy analysts and academic researchers each pursued their work, for the most part, in isolation. With a few exceptions, there has been no concerted effort to build a formal institution bridging the academic and policy systems and, moreover, no effort to study, in the same institutional context and using the same conceptual framework, both security and the changing social context of Canada. We believe these issues must be seen as interconnected and that specialists in each area must learn from the "other side."

We have found that addressing the issues of terrorism, security and society *necessitates* an interdisciplinary approach and a partnership strategy. No academic discipline, no single branch of government, and no civil society organization could legitimately claim ownership over the wide range of knowledge and policy issues related to security and human rights. From our earliest conversations, therefore, we have always based our idea of TSAS in a partnership framework.

One of our first events, held just a few months after we were established, was titled "Collaborative Research Design and a New National Research Community," took place in Ottawa, and was designed to introduce TSAS as an organization and to showcase our determination to work collaboratively with our partners in the policy community. The first half of the day revolved around TSAS researchers explaining their interests and research methods, while the second was devoted to presentations by government officials on their research priorities. The goal of the event was to find points of intersection between scholars and policy analysts: to chart a path that would ensure that knowledge generated by TSAS researchers would not only reach the policy sector but also speak directly to its concerns. This is emblematic of our broader approach.

We place the practice of collaboration at the core of our activities, which we hope will build a culture of policy–research partnership. Our understanding of collaboration is based on our conviction that policy–research partnerships are most productive when they are built upon ongoing dialogue between stakeholders, in our case between academic scholars and people responsible for policy development. Our goal is to move beyond the received model whereby researchers build their projects on pre-defined priorities of government agencies ("give us the questions, give us money, and we'll do the job"), and instead to initiate dialogue that cooperatively shapes those priorities. We are also in accord with the ideas advanced by Peter Checkland (1999; also see Mark Slater's 2013 introductory essay in *Research Methods in Critical Security Studies*) in his exploration of soft systems methodology, where he advocates shifting from pre-defining research methodologies to the adoption of methodological *processes* that enable policy–research teams to react flexibly to changing circumstances through ongoing conversation that can shape and adjust methodologies.

However, while TSAS research is mindful of the priorities of government and brings government officials into our research process, our research agenda is independent. All of our projects are based on our determination to understand and evaluate policy *through evidence*. At times, evidence supports policy decisions that have been made, but some of our projects challenge current policy orientations. We believe, in fact, that this independence is one of the most desirable features of TSAS.

Just two years since TSAS was established, we are seen as a major reservoir of talent, with a *real, demonstrated capacity* to build and mobilize policy-relevant knowledge. Over the last two years we have established several ways to communicate, internally among the approximately 100 researchers affiliated with TSAS, and externally with our partner agencies in government and civil society. We have found that targeted workshops are one of the best mechanisms to facilitate the multi-directional conversations TSAS tries to foster. This book has emerged out of one of these events, titled "Turning a New Leaf: Developments in Research and Policy on Terrorism and Counter-terrorism," which brought over 50 individuals together, enabling informed dialogue between people in sectors that rarely come into contact (for example, those who monitor financial transactions; those who assess the security risk of people who apply for a visa to visit Canada; and those who are responsible for the safe disposal of nuclear waste).

The workshop brought together a mix of established and emerging scholars, Canadian and international researchers, and policy officials, in order to focus on the lessons that social network analysis might bring to the study of terrorism and security. As such, it fit perfectly with the larger TSAS agenda of linking together the understanding of security and society. It was also a highly interactive occasion, structured around TED-talk-like presentations with ample time for conversation between those with theoretical/empirical and policy/operational expertise. Keeping with TSAS's mission of fostering dialogue between the policy and the academic worlds, all panels had a discussant leading the question-and-answer

sessions, and all of those discussants were government representatives whose work was directly related to the themes of the panel. Both sides showed that they were deeply engaged in establishing mutual understanding and trust—key elements for better and more rewarding collaborations.

We believe this book captures the added value gained through these discussions. The contributions are current and innovative and, most importantly, they speak directly to the pressing issues of national security today.

References

Checkland, P. (ed.) (1999) *Systems Thinking, Systems Practice*. Chichester: John Wiley and Sons.

Slater, M. B. (2013) Introduction. In Slater, M. B. and Mutlu, C. E. (eds) *Research Methods in Critical Security Studies*. Abingdon: Routledge, pp. 1–14.

1 Radical and connected

An introduction

Martin Bouchard and Philippa Levey[1]

It is easy for the outside observer to make the connection between radicalization and the Internet. After all, so many of the homegrown terrorists making headlines have been involved in online discussion forums, blogs and social media outlets, while having reported being "self-radicalized" and finding inspiration through watching videos on YouTube as well as reading violent literature found on extremist websites.

Yet, things are usually more complicated than that. First, the Internet is a tool for motivated individuals to search for information and exchange with other like-minded individuals sharing similar interests on any topic (Rainie and Wellman, 2012). It should therefore be no surprise that the Internet is similarly used by would-be terrorists, alongside the much larger crowd of curious observers who are online because of their general interest in exchanging on current world affairs or religion – individuals who should not be confused with "radicals." The baseline hypothesis should then be that extremists use the Internet just as much as anyone else, and as researchers we should therefore investigate the instances where they use it more, less, differently or with more serious consequences than expected.

Second, the Internet is unlikely to be the sole medium of influence for the majority of terrorists. As mentioned by others before us, use of the Internet only gets you so far: far enough for the majority of individuals who may participate in online discussions or view content of an extremist nature but never truly "radicalize" themselves (McCauley and Moskalenko, 2008); not far enough for individuals who are joining terrorist groups engaged in planning and committing violent acts. The latter need offline interactions to further engage in the process, to learn specific techniques, and to start participating in conspiracies (Sageman, 2004, 2008; Awan, 2007; Jenkins, 2011; Nash and Bouchard, this volume).

The reality is that online interactions and material should be considered a key element in the radicalization process of many individuals. Because the Internet is omnipresent in the life of young people, but also because the size, intensity, ubiquity and sometimes quality of the motivational material found online is naturally framed to inspire its target audience, the question then becomes: can it be a sufficient condition for the violent radicalization of individuals? Can the radicalization process start, develop and mature solely online? These remain research questions that can be examined empirically, but despite a growing literature on

this very topic (see Ducol, this volume), the role of the Internet has not been investigated systematically enough to give us clarity on the current situation.

Third, sometimes obscured from the discussions on the role of the Internet in the radicalization process is perhaps the most fundamental question, or the one with the most consequences: does the Internet "create" violent radicalization (and terrorism) where radicalization does not exist? In other words, are there more radicalized individuals because the Internet exists as a communication medium? This is a question also being asked in criminology more generally for many types of crimes, in the cyber context (are there more pedophiles because child pornography is readily available on the Internet?) but also offline (are more individuals becoming drug users in areas where drugs are more available?). This is an exposure argument whereby the availability of online material (violent or extremist in nature) and the possibility of interacting with similarly minded individuals in a virtual community provide an opportunity for radicalization to individuals who otherwise might not have considered this path (Neumann, 2013). These individuals would not have been proactively seeking information on their own. Instead, they would have stumbled upon these ideas for the first time during their routine online activities.

While the possibility of a personal radicalization process occurring solely on the Internet cannot be rejected, it may not be the most common pathway for current terrorist and those of the recent past. The Internet may act as a facilitator and conduit for radical views online, but rarely as an all-encompassing creator of radical offline behavior. The missing element, for many scholars, is the deep friendships of trust that develop as a result of face-to-face interactions evident in small groups (Sageman, 2004, 2008; Awan, 2007; Jenkins, 2011; McCauley and Moskalenko, 2008; Horgan, 2008). This research shows that personal grievances are common among radicals; however, the difference between all individuals with similar grievances and the ones who violently radicalize is often found in the differential socialization of the latter within radical groups (for a summary, see Bouchard and Nash, this volume).

Even if the importance of social ties in the radicalization process is increasingly acknowledged by terrorism scholars, the exact mechanisms under which this occurs have been given less attention. McCauley and Moskalenko (2008) discuss these various mechanisms, such as the slippery slope where individuals gradually become involved with a group, taking on small tasks and actions before complete adherence and membership ensues. More commonly, the mechanism that scholars have in mind, and that radicals are describing, refers to the implications on personal behavior of group cohesion and solidarity to friends. Face-to-face interactions and engagement in group activities provide those involved with a sense of emotional belonging to the group, creating pressure for conformity to group norms and behavior. These sorts of group-level factors are not unique to the context of extremism and terrorism. For instance, group processes help explain why street gang members commit more crime than other offenders but, more importantly, why many are ready to risk serious personal injuries and death for group-level grievances (e.g., Bouchard and Spindler,

2010). Cohesive groups have a tendency to isolate themselves from the rest of the world, cutting most out-group ties held prior to their radicalization (Sageman, 2004). They are, in essence, trading one network for another (Horgan, 2008). The case study of Omar Hammami analyzed in the chapter by Nash and Bouchard in this volume provides a clear demonstration of how a person's pre-radicalization network gradually gives way to a more cohesive network of radicals.

Developments in the understanding of the importance of social networks and the Internet in terrorism are used in this book as a backdrop to propose a relatively wide-ranging set of contributions. The title of the book reflects our objective to cover a wide-ranging set of issues in the field while specifying the importance of social networks in our interpretation of the individual contributions to this book. The sub-title of the book, *Radical and Connected*, captures in two words many of the elements that introduce the nature of the contributions included in this volume. While the word "radical," and its importance for the book, is not mysterious by now, it is the word "connected" which carries with it much of the common thread that can be found in the chapters of this volume. "Connected" in the sense that some of the attention of our authors is devoted to the Internet as a medium of influence for many individuals, whether they belong to the "radical few" or the much larger population of online sympathizers.

But more to the point, these individuals are connected in the sense of "social networks": social networks of terrorists, on the one hand, but also social networks of the agencies organizing responses to terrorist acts and planning for the risks of such events. These agencies are connected as well. They are connected to the Internet, where their investigations inevitably lead them given the importance of computer-mediated communications for terrorist groups and violently radicalized individuals (Sageman, 2004; Neumann, 2013; Soriano, 2012). But they are also connected to other agencies in the context of multi-jurisdictional investigations and/or task forces specifically devoted to terrorist groups (Dupont, this volume; Kitchen and Molnar, this volume). Moreover, they are connected within their own ranks, where issues of internal relations and cooperation never cease to be both a challenge and a source of potential benefit when efficient networking leads to better organizational outcomes. It may not take a network to fight a network (Dupont, this volume), but it takes a team that can effectively cooperate, share information, trust one another, avoid internal conflicts, and work towards similar goals.

Research on cooperation in small groups has consistently shown how the manner in which individuals connect and cooperate have implications for group performance. This is true of terrorist groups whose structure influences the lethality of their attacks (Heger *et al*., 2012) and their ability to avoid detection (Helfstein and Wright, 2011), but also of security and law enforcement agencies (Brewer, 2013; Dupont, 2006; Whelan, 2014). For example, Whelan (2014) interviewed 20 upper-level security officials comprising Australia's national security division for the purposes of examining the internal structural and organizational design of their network. Such a design is said to be most effective at

managing and preventing security-related incidents when high levels of collaboration are present within the network structure (Whelan, 2014). In a similar fashion, Kitchen and Molnar (this volume) examine Canada's counter-terrorism strategy with the goal of observing the effects of integration among social agents (people at all levels of government as well as civilians and foreign partners) and the sharing of national security technological devices. Park and Tsang (this volume) offer some intriguing insight into the recent computational frameworks being designed and tested as a means of identifying the most efficient and effective security responses when faced with possible terror attacks. In the spirit of integration, Kitchen and Molnar (this volume) address the benefits and possible complexities associated with high levels of integration in a manner consistent with Dupont (this volume), who further elaborates on the tension between collaboration and competition among national security organizations within Canada.

The point of departure of this book is the assumption that integrating network concepts and network methods to the study of terrorism and counter-terrorism is of central importance, from theoretical, empirical, and policy perspectives, in bringing the field forward. This is not exactly a new idea, although the move to study terrorist networks did not truly take off until the events of 9/11 (Krebs, 2002). Not all studies in this volume adopt a pure network approach or even use its methods. But all have a deep concern for examining the nature and impact of social interactions and cooperation in shaping the trajectories of terrorists and the nature of the responses to the threat of terrorism.

The organization of the book

Two characteristics make this collection of original papers stand out compared to others. First, it includes scholars from a wide range of disciplines, from the more traditional international studies, sociology and political science to criminology, history and computing science. What we gain in knowledge from the diversity of points of views and training of our authors, we may lose, to a certain extent, in specificity and depth. At the same time, we strongly believe in the need for a book that reflects such a wide variety of approaches under a single cover, as this allows for a broader understanding of the implications of the topic at hand, notably via the natural cross-disciplinary learning that is bound to occur.

Second, this book focuses on a wide spectrum of the possible research themes in the field, as opposed to a single one. The book title reflects this diversity of interest among authors, where new developments in research on radicalization and terrorism are found alongside work on counter-terrorism. The book is divided into two parts. Part I covers issues in radicalization, from the angle of history, network trajectories and the role of the Internet. Part II moves to issues in counter-terrorism, providing critiques of some of the current policies, but also describing some of the promising approaches currently being developed. A common thread among the majority of those contributions is a concern for examining social networks—either as an analogy, a concept, an explanatory variable

or an object of inquiry. Each author accomplishes this in his or her own way, whether small or large, reflecting the relative place social interactions and cooperation have in the work they have chosen to feature in this book. It will be obvious to the reader that no framework was imposed on authors when inviting their respective contributions to this book. The freedom authors received was given in exchange for the meaningful contributions they could provide as experts in their own sub-fields of terrorism studies.

In Chapter 2 André Gerolymatos reminds us how revisiting the history of political Islam can help us better understand the different incarnations of the threats evident today and the security challenges we currently face in the twenty-first century. The social movement around "political Islam" that we see today has its roots in the Ottoman empire of the fifteenth century. This is a story merging the political struggles, religion and identity of Muslims around the world and the perception among some that they belong to one global network where the battles of some are the battles of all. This sort of interdependence is a key idea when understanding the local and global consequences of counter-terrorism policies. After this voyage into the roots of modern terrorism, Laura Huey brings us back to the present in Chapter 3 with her essay on how we approach the study of domestic radicalization. In reviewing recent cases of radicalized Canadians who do not fit the expected profile of terrorists (e.g., such as second-generation converts), Huey demonstrates how standard methodological tools overlook the unexpected cases; ignoring those outliers or "grey swans" puts us at risk of missing valuable and informative information on the process of radicalization. This essay is especially timely in light of the two separate events of October 2014 in St-Jean-sur-Richelieu and Ottawa, where two Canadian converts each killed a member of the Canadian military.

This book argues that attention to social networks is key to the development of the field, and the following contributions make this argument explicit. First, Bouchard and Nash devote a full chapter to reviewing the recent research in terrorism and counter-terrorism using network methods. Their chapter is meant to demonstrate the utility of network methods but also to highlight some of the areas in which additional work is required. The authors clarify the difference between network concepts and network methods and situate the development of network analysis in the wider context of research on radicalization, both online and offline. The next chapter can be seen as almost a response to the first, as the authors move from the conceptual to the empirical analysis of social networks. The contribution by Nash and Bouchard examines the network trajectory of a homegrown terrorist, Omar Hammami. This chapter, more than any other in the book, draws from network methods. Omar's autobiography and other sources were used to recreate the social structure around Omar at six points in time, based on his travel to six different locations: Daphne, Toronto, Alexandria, Mogadishu, Chiamboni and Baraawe. From these six locations, 71 contacts were extracted as part of his network at any one time, divided between family ties, friends, jihadi brothers, jihadi leaders and religious/teacher influences. The authors show how Omar's network significantly changed from one location to

the next, depending on his ability to branch out from the highly connected clique he usually integrated upon his arrival. Friendship and family ties gradually disappeared to favor jihadi brothers, and especially jihadi leaders in the last two parts of his journey in Somalia.

The next three chapters move the discussion to issues surrounding terrorism and the Internet. First, Benjamin Ducol reflects on radicalization, showing that to understand the impact of the Internet on radicalization processes it is imperative to grasp the impact that both online and offline communities have on behavioral outcomes. Such an interaction effect is made more complicated by the ever-changing nature of the Internet, especially taking into account the change in the participants who now have access to, and control over, this communication tool. Ducol addresses the complexities and dangers of assuming radicalization to occur by means of a single factor in isolation, and he elaborates on the importance of integrating offline behaviors and cognitive developments supporting radical beliefs with online activities. The chapter by Davies and colleagues approaches the notion of terrorism and the Internet by examining recruitment processes employed by extremist and terrorist groups through official online websites. Alongside a typological analysis of four online recruitment styles, the inconsistencies of recruitment tactics and use of social media between groups allows for a thorough discussion on the extent to which extremist groups use the Internet to achieve their own ends.

The importance of examining both online and offline extremist behaviors is also emphasized by Thomas Holt and colleagues, who presented the results of a cross-country survey examining the factors predicting the willingness of individuals to commit attacks online and offline. The potential for cyberterrorist attacks have been identified for a long time, and yet empirical research associated with cyberterrorism is scant. The research results show that the profiles of these "cyberwarriors" overlap considerably with those of traditional online communities of cybercriminals. Out-group antagonism, in particular, was associated with a higher willingness to carry out attacks both online and offline.

Part II of the book covers a variety of issues in counter-terrorism. In Chapter 9, Benoît Dupont argues that the commonsensical and widely accepted idea that "it takes a network to fight a network" is fraught with a host of risks that are rarely considered in counter-terrorism policies. The author does not deny the benefits of flexible partnerships, reciprocal information flows and increased cooperation more generally, but he reminds us of some of the incompatibilities of network structures with the actual mandates of counter-terrorism agencies. The subsequent chapter pushes further this critical assessment of the organization of the response to terrorism. Reflecting on the tendency of counter-terrorism institutions (and Canada's counter-terrorism strategy) to integrate multiple agencies, Kitchen and Molnar suggests that although integration is often presented as "the" answer for such task forces, it solves only a silo problem but may lead to new inefficiencies, increased complexity and diffused accountability. The authors also see promises in integration and cooperation if the process is done correctly. Accounts of units emphasizing joint training events and other

opportunities for social interactions among members have shown increased cohesiveness within integrated units and the reduced tensions that naturally arise in such contexts.

Finally, in Chapter 11 computer scientists Andrew Park and Herbet Tsang provide us with a fascinating glimpse into the future with a presentation of the latest research on simulation models created to help answer some of the "what if" questions regarding individual and group dynamics in the event of a terrorist attack. As artificial as the world created by these scientists may initially seem, the utility of these simulation models for the sound planning of interventions and crisis management will appear extremely concrete to any reader. The manner in which our nations respond when faced with attacks of terror and violence has direct consequences for the general public and first responders. Such a computational model as the one explained in this chapter allows us to take one step closer to this end goal.

Note

1 Martin Bouchard would like to thank Philippa Levey, Evan Thomas and Marie Ouellet for their assistance in preparing the final version of this volume as a whole. As Daniel Hiebert and Lorne Dawson mention in the Foreword, the idea for this book started in the context of a TSAS workshop where many of the individual contributors presented their work. Martin would like to thank Dan and Lorne for their encouragements and continued support, as well as Brett Kubicek for his leadership in the creation of the TSAS environment. The staff at TSAS who originally helped in the preparation of this book include Kate Castelo, Vicky Baker, Marit Gilbert and Marni Wedin. TSAS itself was originally created from a partnership grant between Public Safety Canada and three universities: University of British Columbia, Simon Fraser University and University of Waterloo. I would like to thank them all for their support and at the same time remind readers that the views expressed by the contributors of this book do not represent those of any of these institutions.

References

Awan, A. N. (2007) Radicalization on the Internet? The virtual propagation of jihadist media and its effects. *RUSI Journal.* 152 (3), pp. 76–81. DOI: 10.1080/03071840701472331.

Bouchard, M. and Spindler, A. (2010) Groups, gangs, and delinquency: Does organization matter? *Journal of Criminal Justice.* 38 (5), pp. 921–933.

Brewer, R. (2013) Enhancing crime control partnerships across government: Examining the role of trust and social capital on American and Australian waterfronts. *Police Quarterly.* 16 (4), pp. 371–394.

Dupont, B. (2006) Delivering security through networks: Surveying the relational landscape of security managers in an urban setting. *Crime, Law and Social Change.* 45 (3), pp. 165–184.

Heger, L., Jung, D. and Wong, W. (2012) Organizing for resistance: How group structure impacts the character of violence. *Terrorism and Political Violence*. 24 (5), pp. 743–768.

Helfstein, S. and Wright, D. (2011) Covert or convenient? Evolution of terror attack networks. *Journal of Conflict Resolution*. 55 (5), pp. 785–813.

Horgan, J. (2008) From profiles to pathways and roots to routes: Perspectives from psychology on radicalization into terrorism. *Annals of the American Academy of Political and Social Science.* 618 (1), pp. 80–94.

Jenkins, B. M. (2011) Stray dogs and virtual armies: Radicalization and recruitment to jihadist terrorism in the United States since 9/11. Rand Corporation.

Krebs, V. (2002) Uncloaking terrorist networks. *First Monday*. 7 (4).

McCauley, C. and Moskalenko, S. (2008) Mechanisms of political radicalization: Pathways toward terrorism. *Terrorism and Political Violence*. 20 (3), pp. 415–433.

Neumann, P. R. (2013) Options and strategies for countering online radicalization in the United States. *Studies in Conflict and Terrorism.* 36 (6), pp. 431–459.

Rainie, L. and Wellman, B. (eds) (2012) *Networked: The New Social Operating System*. Cambridge MA: MIT Press.

Sageman, M. (ed.) (2004) *Understanding Terror Networks*. Philadelphia: University of Pennsylvania Press.

Sageman, M. (2008) *Leaderless Jihad: Terror Networks in the 21st Century*. Philadelphia: University of Pennsylvania Press.

Soriano, M. R. T. (2012) The vulnerabilities of online terrorism. *Studies in Conflict and Terrorism.* 35 (4), pp. 263–277.

Whelan, C. (2014) Managing dynamic security networks: Towards the strategic managing of cooperation, coordination and collaboration. *Security Journal*. DOI:10.1057/sj.2014.20.

Part I

Terrorism and radicalization

History, networks and the Internet

This page intentionally left blank

2 The roots of terrorism in the Middle East[1]

André Gerolymatos

Introduction: Islam and the War on Terror

Historical injustice and the unity of Islam constitute the bedrock of the ideological arsenal of the modern-day jihadists. An understanding of the grievances of the late nineteenth and twentieth centuries and of the desire to unify the Muslim world offers considerable insight into the forces that motivate the terrorists (or jihadists) who claim to wage a holy war in the name of Islam. In this context the concept of "jihad," or holy war, literally meaning "struggle," has become synonymous with Middle Eastern terrorism and often manifests in suicide attacks. Although the term has several interpretations, such as an internal and spiritual effort against sin or temptation, it has also been understood by Muslim extremists to mean the armed struggle to counter persecution and oppression and to wage war against the enemies of Islam. The holy war version of jihad, which figured prominently in the history of the Crusades, in the twentieth century became a recurring theme in the rhetoric of a variety of Muslim extremists and militants. Al-Qaeda and its offshoots, like earlier radical organizations, drew nourishment from the concept of jihad in asserting their right to inflict violence against Islam's foes—mainly the West and particularly the United States. Richard Mitchell, an authority on the Muslim Brothers in the late 1960s, wrote: "Western Imperialism crusading … appeared as an attempt not only to conquer Muslim lands but to subvert Muslim society—in effect, cultural as well as military domination of the Islamic world by the West" (Mitchell, 1969, p. 229). The *raison d'être* of contemporary jihadists echoes the plight of Islam during the period when Britain, France, Russia and Italy controlled most of the Muslim world, with the exception of Turkey. At this time, Islam and Islamic institutions adapted to non-Muslim masters, but when colonialism came to end in the post-Second World War period, Muslim leaders and their organizations had to re-adapt to a new political environment—one dominated by a tidal wave of secular nationalism and later by forces trying to reorganize a postcolonial Islam. An underlying reason that the postcolonial period remains tumultuous is, as Abbas (2014) notes, the difficulty that Muslims and Muslim organizations have in coming to terms with Islam and its relationship to nationalism.

In effect, from the early 1950s until the death of Gamal Abdel Nasser in 1970, the vast majority of Muslims looked to the Egyptian strongman as a messiah to lead them to dignity, prosperity and a return to Islam's Golden Age. Nasser was the dominant force in the Middle East and represented almost a secular caliph. His death, the continued defeat of the Arab armies at the hands of the Israelis, and endemic corruption and poverty shattered the notion of a secular solution to the woes of the Muslims. The Ayatollah Khomeini's revolution in Iran, and the success of the *mujahidin* in defeating the Soviet empire in Afghanistan brought to the forefront the transformation of Islam into a political force and the reimagining of Muhammad's "pure Muslim society." The practitioners of Muslim terrorism in the Middle East take inspiration from the unifying force of Nasser's pan-Arab leadership and in the form of political Islam aim to recreate the unification of the Muslim world under a caliphate. Consequently, an examination of the period just before and after the First World War sets the context for the fermentation of grievances that spills over to the postcolonial era after 1945. The emergence of Nasser, to a great extent, is the culmination of nationalism and the movement for Arab unity, although his failures serve as a preamble to the short-term rise of secular radical organizations—only to be superseded by the jihadists, who look to Islam and the reestablishment of the caliphate for a Muslim unity imagined to have existed in the time of Muhammad.

Historical background

The "Arab Street," the anonymous masses that make up the urban poor, feeds on the retelling of a variety of conspiracy stories. The most important recurring theme is the Crusades. At the end of the twentieth century, the notion of the Crusades as a grand conspiracy of the West against the Muslim world received new impetus when in 1990 US president George Bush, Sr. proclaimed "a new world order." Although Bush's remarks referred to the post-Cold War era in the Middle East, the writer Daniel Pipes states that in the region, "the phrase was widely understood as signaling a plan for 'the United States, master of the new world order' to establish hegemony over the entire globe" (Pipes, 1996, p. 110). Hence Middle Eastern perceptions point to the "new world order" as further evidence of a policy of "crushing Islam and its people [and] a Jewish plan for a Greater Israel and a Christian 'spirit of the Crusades'" (Pipes, 1996, p. 110). Osama bin Laden frequently used the terms "Crusaders" and "Crusade" in his characterization of the West and the presence of the US military forces in the Middle East. President George W. Bush Jr. inadvertently reinforced this notion in the Middle East in a speech on the future course of American policy eight days after 9/11, when he labeled the war against terror (what essentially would be a series of intelligence and covert operations) a Crusade against terrorism. This statement invoked the specter of a religious, as well as secular, conflict with Islam.

The War on Terror, like the Crusades, is waged without recourse to the rules of war. Although Western medieval armies fought, more or less, under a set of self-imposed regulations, these applied only to fellow Christians. The Geneva

Convention, and the interpretation of it by nation-states, inadvertently replicates this issue; the rules of war in the twentieth and twenty-first centuries, while almost universally accepted, were designed for conventional warfare. As a result, the Geneva Convention did not make provisions for covert operations or espionage.[2] For jihadists, war against the Western infidels is by its very nature devoid of any recourse to rules or the humanitarian treatment of non-combatants. For militants, in fact, war against the West necessitates both civilian as well as military targets.

An important factor in the emergence of modern Muslim militants is that Western intelligence organizations, and not transparent government agencies, had responsibility for dealing with Muslim extremists. Indeed, in the twentieth and twenty-first centuries, both Anglo-American and Axis intelligence organizations, later followed by the Soviets, recruited Muslims to radicalize the other country's Muslim minorities. In the First and Second World Wars, necessity created the momentum for a secret relationship between the intelligence services of Great Britain (and later the United States) with the emerging Islamic radical movements and religious zealots such as the Muslim Brotherhood. The Anglo-American secret services desperately needed agents to use, first against the Ottomans, later against the Axis, and finally as a means to contain the rising Arab nationalism that British operatives such as T. E. Lawrence had helped to instigate in 1916.

Ironically, on the eve of the First World War, except for those parts of the Middle East that had been colonized by the Europeans, the remaining predominantly Muslim regions were under the shaky control of the Ottoman Empire. The Ottomans, a disparate assortment of Turkish Muslim converts, had gravitated from Central Asia as mercenaries for various territorial entities and in time evolved into a formidable army that swept away the remnants of the Byzantine Empire. The Ottomans conquered the great city of Constantinople in 1453 and by the next century had spread out from the Balkans and Asia Minor to envelop most of the Middle East. The Ottoman armies proved unbeatable by contemporary powers. By the sixteenth century, they had conquered most of North Africa, all of southeastern Europe and parts of Hungary and had brought their armies to the gates of Vienna. A century later, however, Ottoman supremacy had been eclipsed by the European powers, and the empire began a long and irreversible decline until its final demise after the end of the First World War, formally ended by the Turkish parliament under the direction of Mustapha Kemal (Ataturk) on 3 March 1924 (Mango, 2010). The Great Powers, particularly Britain, had been convinced that the collapse of the Ottomans would create a political vacuum in the Middle East that would be exploited by other powers, particularly Russia, and they undertook to prop up the Ottoman Empire for much of the nineteenth century. As long as the Ottoman Empire remained more or less intact, the sultan, with the backing of the Royal Navy, could maintain Turkish sovereignty over the Straits and thus deny the Russian Black Sea fleet access to the Mediterranean. In addition, with the British and French propping up the Turks, the remaining provinces of the Ottoman Empire could be denied to the Russians. Yet despite the weakness of the empire, the sultan, as caliph, continued to represent the unity of Islam that extended to Sunni Muslims throughout the world.[3]

In the early twentieth century, the prospect of a mass uprising of Muslims after the sultan-caliph declared a jihad had fixated the Germans and British, who expended considerable nervous energy and gold on stimulating or preventing a future holy war. Before the First World War, as Lüdke (2005) argues, the Germans had established a pan-Islamic propaganda office in Berlin, which focused on Islamic issues in the Ottoman Empire and in the territories of the Entente that included large numbers of Muslims. The British, for their part, had concentrated their efforts on the Sharif of Mecca as a possible antidote to counter the Ottoman Sultan's proclamation of holy war.

British strategy was strengthened by the fact that by the end of the nineteenth century the Ottoman sultan's monopoly of the position of caliph was facing legal and secular challenges from within the Muslim world. Authoritative Islamic scholars Hourani (1962) and Hagen (2004) argued that the Caliphate should be reformed and restored to an Arab chieftain.[4] Ibn Saud, the Emir of the Nejd and head of the puritanical Wahhabi sect, rejected outright the idea that the sultan's role as Caliph gave him secular authority over the Muslim community world-wide. The British, for their part, as Peters (1979) states, successfully countered the possible impact of the sultan's jihad by securing opinions from Islamic legal experts and Muslim clerics in Egypt and India, who asserted that it was the obligation of Muslims to obey the British authorities. Rudolph Peters, on the other hand, concludes that the main reason for the failure of the jihad:

> was that Pan-Islamism lacked any form of political mass organization. Despite the exaggerated notions with regard to its force and impact prevalent in Europe, Peters argues it was no more than an idea espoused by some intellectuals as a reaction against the rapid spread of Western domination during the last quarter of the nineteenth century.
>
> (Peters, 1979, p. 94)

Regardless of the collapse of the jihad, the fear of a pan-Islamic movement inflamed by religious fervor in an all-out holy war continued to haunt and intrigue the British, and later American strategists into the twenty-first century.

In 1914, the Ottomans chose to link their fortunes with imperial Germany in a desperate bid to re-acquire lost territories and past glories, and the sultan declared a jihad against the Entente powers in November. Critical to the success, or failure, of this call to the faithful was the Ottoman Empire's Arab population. Consequently, the Allies—particularly the British—saw in the Arabs the key to countering the influence of the Ottoman sultan as caliph and his prerogative to declare a jihad. The notion of a holy war instigating a massive uprising of Britain's Muslim subjects dominated the thinking of British officials in Whitehall and Cairo. The Germans were equally interested, but in their case they wanted to convince the Ottoman ruler to declare a jihad in a future war with the Entente. Nevertheless, despite the fears and hopes of both sides, neither the Sultan's role as Caliph nor the declaration of a jihad had any significant impact on the war.

By early 1916, the Arab Bureau, Britain's intelligence organization in Egypt, had become the driving force behind Sharif Hussein bin Ali's Arab Revolt. As Sharif of the holy cities of Mecca and Medina, Hussein held a degree of moral and, to some extent, religious standing with Sunni Muslims. It may even be that after the sultan proclaimed a jihad, the fact that the Sharif of Mecca and Medina did not endorse it may have gone some way to ensuring the failure of the call to arms by the sultan. In actual fact, Hussein represented only himself and led an army of Bedouin, whose loyalty was bought with British gold, but this did not hinder the plans of the Arab Bureau for a united Arabia under British tutelage. It suited their interests for Hussein not to lead a substantial Arab force or to head a pan-Arabic mass-based movement, as under these conditions it was far easier to control the Sharif's ambitions and divide the loyalties of the other Arab leaders. The difficulty with this foreign policy, however, was that it was compartmentalized; the British authorities in Cairo conducted a regionally based policy, while the government in London was more concerned with postwar grand strategy.

The Sykes–Picot Agreement of May 1916, for example, concluded in London without the knowledge of the Arab Bureau, complicated the relationship between Hussein and the British and undermined the Sharif's position with the Arabs. The Sykes–Picot Agreement, in essence, divided the Middle East into French and British protectorates—in effect colonies. After the Russian Revolution in October 1917, the Bolsheviks published all secret treaties between Russia and the Entente, including the Sykes–Picot Agreement, in November 1917, to the acute embarrassment of the Anglo-French governments.[5] Regardless of the subsequent debate on what the agreement was meant to achieve, and to what degree the British betrayed or did not betray the Arab Revolt, the reaction in the Arab and Muslim world was negative and Sykes–Picot continues to be regarded as a fraud and a betrayal.[6]

Yet this was not the only disillusionment. On 2 November 1917, the British Government issued the Balfour Declaration, committing Britain to the creation of a Jewish homeland in Palestine. News of the Balfour Declaration, as Antonius (2001) notes, caused considerable unrest and protest among the Arabs and throughout the Muslim world. Together with the Sykes–Picot Agreement, it provided the building blocks for future Muslim accusations of British perfidy and betrayal by the West. Meanwhile, the policy of the Arab Bureau in fostering the notion of a nationalist Arab state was to counter the Islamic identity represented by the sultan-caliph. Regardless of its configuration and the *realpolitik* exercised by the political leadership in London, this policy eventually engendered a duality in the Middle East that oscillated between the pursuit of Arab nationalism and the quest for the re-establishment of an Islamic state.

The division of the Middle East into British and French spheres of influence, as Dawisha (2003) explains, contributed to Arab nationalism and the rise of militant Islam, both of which gained considerable momentum after the First World War.[7] Certainly, the British intelligence community in the region cultivated nationalist and Islamic strains. The Arab Bureau had lobbied for Hussein and Arab nationalism, which they assumed was secular, while promoting the Sharif as an Arab

caliph. Yet, with the exception of Christian Arabs and a small number of intellectuals, Arab nationalism was rooted in Islam. In attempting to play one off against the other, the British unknowingly succeeded in fortifying the Islamic identity of most Arabs. Secular Arab nationalism, except for that led by Gamal Abdel Nasser for a few decades after the Second World War, dissipated in a sea of corruption, poverty and defeat. Ultimately, the failure of secular Arab nationalism fortified the strength of Islam in the region left a difficult legacy for the Middle East, and inspired resentment of the West.

Indeed, the Islamic factor had skewed British policy towards the Middle East both during and after the First World War. Bureaucrats, politicians and intelligence officers in London and Cairo misunderstood religion and nationalism in the Middle East and assumed they could control the former and manufacture the latter. In the decades after 1918, in order to secure their interests in the region, the British and later the Americans attempted to manipulate religion and nationalism by seeking a strong man either as the focal point of Arab nationalism or as the centerpiece of Islamic unity. Muslim scholars and militants in the Middle East, on the other hand, looked for a unifying force to bind their world, which had been disrupted by the end of the Ottoman Empire.

The end of the caliphate and the Muslim Brotherhood

The abolition of the caliphate by the new Turkish Republic in 1924 left a significant void in the Sunni Muslim communities around the world and stimulated several disparate movements that have sought to reconstruct Islamic unity. While intellectuals and politicians alike put forward alternative concepts for Islamic unity, for many Muslims the reestablishment of a new caliphate held the strongest appeal.[8] The Muslim Brotherhood, as Lia (1998) explains, was established four years after the Ottoman caliph was forced to step down; it had as one of its fundamental goals the political unity of Islam through the reestablishment of a new caliphate. Subsequently, the quest for the leadership and the unification of both the international and regional Islamic community has oscillated between the claims of Islamic militants and ambitious secular leaders. Meanwhile, Anglo-American intelligence officers throughout the century assumed that a single master could direct a "monolithic" Islam and that—through him—they could guide events in the Middle East. This assumption, held dear by the British and later by some Muslim experts in the Anglo-American intelligence services, was based on the notion that some kind of entity could assume the unifying role of the caliphate that would hold the loyalty of the Muslims and transcend national boundaries. In contrast, for radical Muslim and Arab nationalists, the struggle against the European hegemony (and later the United States), as well as against those Muslims perceived to be working with the West, had to be waged underground by urban warfare, assassination, propaganda, espionage, subversion and martyrdom through suicide.[9]

Until the appearance of Al-Qaeda in the 1990s, the Muslim Brotherhood carried the banner of radical and—to Western as well as established Middle Eastern

regimes—fanatical Islam. An Egyptian teacher, Hasan al-Banna, created the Muslim Brotherhood, or more specifically the Society of Muslim Brothers, in 1928.[10] The first major activity of the Brotherhood was to build a mosque, school, and clubhouse in Ismailia. Al-Banna raised the necessary funds for the structure from many sources, including £E500[11] from the Anglo-French Suez Canal Company—a symbol of British domination. Ten years later, as Lia (1998) notes, the Muslim Brothers began advocating nationalization of the canal. It is not certain why the Suez Canal Company donated the funds. Later, however, the British had few reservations over tolerating and even supporting an organization that was antithetical to their presence in Egypt. This cynical approach was motivated, in part, because, like the British, the Muslim Brotherhood was also opposed to Egyptian nationalists, left-wing organizations, independent labor institutions, and communist entities in general. The *raison d'être* of the Muslim Brotherhood was—and continues to be—cleansing Islam of all foreign elements and restoring it to its pristine essence as practiced at the time of the Prophet Muhammad. To accomplish this resurrection of the true faith, as Johnson explains, the slogan of the Muslim Brothers was: "The Koran is our constitution. Jihad is our way. Martyrdom is our desire" (Johnson, 2010, p. 110). This mantra is part of the ideology of other Muslim extreme organizations.

The Muslim Brotherhood was just one group that sought to rebuild the unity of Islam that they imagined had existed under the sultan-caliph rather than by the force of the Ottoman armies. Ever since 1924, in one form or another, various Muslim organizations and individuals have been trying to recreate the Islamic unity that they perceive as having been represented by the Ottoman caliph. The search for an all-embracing Islamic entity, through either the leadership of a single religious–political entity, or that of an individual, remains at the crux of the Muslim restlessness that has marked the twentieth century and the early twenty-first. In the early part of the twentieth century various Islamic scholars looked to how a national consciousness could replace the fragmentation of the Muslim world and counter the influence and subjugation of the West. Some, such as Jamal al-Afghani and Mohamed Abduh, advocated, as Esposito (2003) explains, a return to early Muslim ideals. By the 1930s, various Muslim intellectuals were promoting regional nationalism, while others turned to religion and the concept of a transnational Islam that reflected the Muslim world as it was in the seventh century. Although some Muslim activists welcomed the notion of unifying the Arabs, they saw this only as a first step, as Dawisha (2003) argues, to the establishment of an Islamic state to replicate the central role of the caliphate. Their quest for unification and their advocacy of militancy acquired considerable momentum in the clash between the Palestinians and the British in the 1930s.

The road to radicalism

The 1936 Arab revolt in Palestine, led by the Mufti of Jerusalem, al-Husseini, was, as Harris (1964) explains, more than an uprising both in its duration (1936–39) and in its impact on pan-Arabism and on Egypt in particular. The

desire of the Palestinians to free themselves from British rule, notes Dawisha (2003), spilled outside the confines of Palestine and transformed into a cause espoused by Arab nationalists and Muslim militants, as well as by ordinary people in the Middle East. Indeed, the Palestinian struggle eventually became part of the rhetoric of pan-Arabists, militant Muslims and jihadists, and later, for a short time, that of radical and revolutionary groups in the West.[12] The three-year crisis and the eventual defeat of the Palestinians radicalized an entire generation of Arabs and engendered the notion of Egypt as the champion of the rights of all Arabs, thus eventually becoming the home of the Arab League established in 1945. For the Muslim Brothers, argues Harris (1964), their participation in Palestinian struggle elevated the organization from the fringes of society to a rapprochement with mainstream Egyptian political elites.

Morris (2008) contends that the Palestinian crisis of 1936 was neither the first nor the last, but one in a series of violent rebellions that ultimately became a major stimulant to radical movements in the Muslim world in the twentieth and early twenty-first centuries.[13] Arab resistance to the British in Palestine provided inspiration for the rise of nationalism in Egypt. It also helped to instigate pan-Arabism, which many Muslim intellectuals believed would come under Egyptian leadership, thus paving the way for Nasser's revolution of 1952. The Palestinian struggle beckoned secular Arab nationalists, as it did militant Muslims, because it underscored the fight by Arabs in Palestine for self-determination and statehood as well as their war first against Jewish settlers and later against the Israeli state. At the same time, the position of Jerusalem in Islam acted as a magnet for the religious militants, who could not accept the loss of the third sacred city so critical in the Islamic faith. Indeed, the Jerusalem factor added a religious layer to the struggle. The Islamic element, at first subtle, was part of the Palestinian war against the Israelis. Palestinian irregulars who came out of the refugee camps from the Egyptian side of the border and conducted raids into Israel were labeled as the Fedayeen or "sacrificers."

Nasser and Arab unity

The outbreak of the Second World War and the links between al-Banna and the Nazis crystalized the strong ties established between the Muslim Brothers and the virulent anti-Semite al-Husseini, the Mufti of Jerusalem. During the 1930s, al-Banna found common cause with the Nazis in their mutual commitment to anti-Semitism and accepted considerable funds from a Nazi agent affiliated with the German embassy in Cairo. Al-Banna used the money, as Johnson (2010) notes, to establish the "Special Apparatus" a paramilitary offshoot of the Muslim Brotherhood, which he used to support the Arab rebellion in Palestine. Many in the Arab world believed in and hoped for a German victory, and after the war Muslim fanatics and militants such as al-Hussaini maintained links with Nazi agents and former SS officers. During the 1940s al-Banna established contact with a large group of nationalist Egyptian officers, through a young officer named Anwar Sadat. The Free Officers, predominantly colonels in the Egyptian

military led by Colonel Gamal Abdel Nasser, were committed to ridding Egypt of the British as well as King Farouk. Initially the Free Officers and the Muslim Brotherhood shared these common goals and the Brothers supported the 1952 military coup that forced Farouk to abdicate.

The Muslim Brothers, however, became disenchanted with Nasser's secular and nationalist policies. At the same time, the Egyptian leader had come to resent the society's growing influence and opposition to his regime. On 26 October 1954, a member of the Brotherhood attempted to assassinate Nasser. Subsequently, as Mitchell and Richard (1969) recount, the Egyptian strongman turned against the society and the security services proceeded to arrest thousands and executed hundreds of the Muslim Brothers. Sayyid Qutb, the most influential advocate of the contemporary concept of jihad and the spiritual guide for Muslim militants and jihadists, was one of those incarcerated. After another assassination attempt on Nasser, the intellectual father of the jihad was executed on 29 August 1966. For many extremists and terrorists in the Middle East, Qutb's reinterpretation of "holy war" legitimized extreme violent Muslim resistance against governments that claimed to be Muslim but whose implementation of Islamic precepts was seen as flawed. Qutb is especially popular in Saudi Arabia, but his extensive publications have also been translated into languages used by the majority of the world's Muslims.[14] In effect, Qutb is regarded, notes Irwin (2001), as the father of contemporary militant Islam and the inspiration and influence for many terrorists, including Osama bin Laden.

Qutb and the Muslim Brotherhood appealed to hundreds of thousands of young men and women caught up in the post-colonial world of the Middle East, cluttered with vociferous nationalist movements and tugged in several directions by ambitious leaders. For the superpowers, on the other hand, the region offered opportunities for Soviet as well as American strategists who believed that Egypt held the key to the region. Both Nasser and the Muslim Brotherhood, consequently, became caught up in the struggle between Washington and Moscow over the heart and minds of Muslims in the Middle East and throughout the world. US policy-makers in the late 1940s viewed the region as a maze of cross-currents: national ambitions, religious zealotry, and conflicting loyalties. The Americans attempted to find a single strong man who could create order out of chaos and preempt Soviet intrigues in the Middle East. Nasser was a likely candidate—leader of a genuine national mass movement and head of the largest Arab country, which was emerging as the leading state in the region.

In the 1950s, Nasser's ability to avoid the assassination attempts of the Muslim Brotherhood and other groups was partly a direct result of the CIA's activities in Egypt. While one factor in Nasser's continued survival was luck, a more tangible consideration was that Nasser had an exceptionally capable security apparatus, equipped and trained indirectly by the CIA.[15] The agency's involvement with Nasser was a byproduct of the fear of communism that swept across America after the Second World War and transfixed successive US administrations to containing the Soviets. The Truman White House, as well as the Eisenhower government, became interested in Nasser because of the strategic

role of the Suez Canal, the petroleum of the Gulf states, and the fear that British and French colonialism would pave the way for the USSR to gain control of the Middle East. America's record in the region, furthermore was untainted by colonialism and historical injustices such as the Sykes–Picot Agreement, the Balfour Declaration or the post-First World War mandate system.

Nasser, the Americans and the Nazis

Although the Eisenhower administration was not as close to Israel as Truman's, the Israeli factor forced Washington to limit the outward appearance of America's relationship with Nasser. Yet Nasser, for his part, could not wholeheartedly cast his lot with the Americans, because the Israeli factor was too great a chasm to overcome and survive politically. Accordingly, contact between Nasser and the United States evolved on two levels: a formal diplomatic relationship with all its limitations, and much more substantive links carried on clandestinely through the CIA. Furthermore, when the CIA could not directly provide certain services required by Nasser, it was able to use the Gehlen Organization, a CIA-controlled German intelligence group that provided the necessary expertise and personnel, which offered the US Government the fig-leaf of plausible deniability.[16]

From available American documents and secondary sources, it appears that the CIA successfully used the cover of the Gehlen Organization (and later the West German intelligence service) to avoid direct involvement with the actual placement of German advisors in Egypt. Later, however, the CIA established direct links with these former Nazis once they had arrived in Egypt. As Timothy Naftali states:

> the extent of Gehlen's recruitment of former officers of the SD [the security service of the SS] and Gestapo … was widespread. At least one hundred of Gehlen's officers and agents had served with the SD or the Gestapo, and the number may in fact be significantly higher—some of those hired had participated in the worst atrocities committed by the Nazi regime.
>
> (Naftali, 2005, p. 377)

The CIA did facilitate the arrival of former German military and security personnel to Egypt; some of the Germans, including Wilhelm Voss, had arrived before 1953 at the invitation of King Farouk. General Wilhelm Fahrmbacher led one of the first groups, numbering about 30 officers, to Egypt in 1950.[17] Most were career soldiers hired by Farouk, who always had had a soft spot for the German Africa Corps, to replace the British Military Mission, which had left Egypt in 1947. Economic, industrial and administrative experts followed shortly before and were joined, in turn, by missile and aircraft engineers and other weapons scientists.[18] An additional one hundred "advisors" were dredged from their hideouts in Germany, South America and Spain and made their way to Egypt along the ratlines operated by various neo-Nazi escape organizations.[19] One of the most contentious activities that the ex-Nazi officers were engaged in was the

training of Muslim Brotherhood paramilitary units in guerrilla warfare prior to the break between the society and Nasser ("Egyptian soldiers learn the German way," 1953).[20]

In December 1952, the Egyptian government announced the formation of a labor service aimed at providing discipline and employment for students, which included a paramilitary wing, the "Liberation Battalion." As the Liberation Battalion training camps were established, the Egyptian government launched a highly publicized recruitment campaign. According to British reports, about 10,000 individuals were trained in these camps, but

> of these … possibly as many as 6,000 have been members of the Moslem Brotherhood who have taken advantage of the training offered in Government-organized camps without in any way transferring their allegiance to the Liberation Rally from the squads of the Moslem Brotherhood.
>
> (Hankey to Salisbury, 1953)[21]

Muslim Brotherhood cadres were indeed participating in the government camps. After the January 1952 Egyptian officers' coup, existing guerilla organizations, including those of the Muslim Brotherhood, were disbanded. Nevertheless, a large number of the Muslim Brothers, with a wealth of experience in underground warfare, had by the end of 1952 volunteered and resumed training.[22] From this point onward, Muslim Brotherhood recruits generally attended the Liberation Battalion camps for initial training—although the Muslim Brotherhood maintained its own secret training camps for the "final preparation" (Egyptian Para-Military Forces, 1953) of its members.[23] These volunteers, recruited from university were organized into three categories: unattached men, men with no dependents, and men with dependents but no children. The same British report states: "The most dangerous assignments will be allotted to men in the first category, who may well act as 'suicide' squads" (HQBTE Report, 1953).[24] It was estimated that, in addition to the existing units, approximately 8,000 men had been trained in the Brotherhood's own camps but not yet formed into squads (HQBTE Report, 1953).[25]

The German advisors were certainly involved in training at all the government camps, but their presence seems to have been much stronger in the predominant Muslim Brotherhood facilities, as well as in the Liberation camps that had been set aside for the training of the society's members.[26] A May 1953 British report notes evidence of "considerable assistance" being given to the Brotherhood's paramilitary arm (IEM Kateibas) by German advisors. It went on to state that:

> In particular a great deal of attention has been paid to [training] in explosives, demolition, sabotage, etc. which will be a feature of IEM operations. IEM Kateibas are being trained by expert German advisors for specialist sabotage tasks. Such targets as filtration plants, 9 BAD, armouries, Main HQs and communication centres are likely to be the object of carefully

> timed and planned sabotage operations for which specific training and even rehearsals have been undertaken with meticulous German thoroughness.
>
> (HQBTE Report, 1953)[27]

A later report explained:

> There has certainly been considerable German influence if not assistance in training. This has given rise to increased attention being paid to and probably more effective techniques in the use of explosives, sabotage and in mobile Commando type operations. Such assistance is probably more apparent at IEM than at Liberation unit establishments.
>
> (HQBTE Report, August 1953)[28]

The Muslim Brotherhood's volunteers were not only being trained separately in guerrilla warfare tactics; they remained ideologically segregated from the government units. In Lord Hankey's view, the Muslim Brotherhood would not cooperate with the Liberation forces in a clash with foreign forces; he argued: "it is unlikely that they would now agree to pick the chestnuts of the [Egyptian government] out of the fire" (HQBTE Report, 1953).[29] It was understood by the British that the Brotherhood remained a "more formidable proposition" than the regular Liberation Squads, particularly as they had "been able to take advantage of training in Government camps without losing their identity" (HQBTE Report, 1953).[30] The CIA had helped to engineer this state of affairs, regardless of the ramifications for the future. It is not certain if the CIA's covert support of the Muslim Brotherhood was to help Nasser with his struggle against the British, or if the American intelligence agency also saw in the Muslim Brothers a means by which to checkmate the Egyptian dictator.

In the immediate period after the overthrow of Farouk, Nasser had remained behind the scenes and General Muhammad Naguib was declared president, but the young colonel had the loyalty of the Egyptian officer corps and continued to wield considerable influence within the military. Although Nasser had been instrumental in elevating Naguib to the presidency, the two men quickly grew apart. Naguib believed in reforming Egypt's institutions, including the monarchy, while Nasser advocated radical changes, such as a significant land redistribution that would lead to a social revolution. To stay in office, Naguib sought alliances with the Muslim Brotherhood and the United States, but beyond hanging on to power, he stood for very little and, more importantly, did not have the backing of a local organization. Nasser had the loyalty, as Aburish (2005) states, of the officer corps; in time, he would secure the adoration of most Egyptians and of the Arab world.

In 1954, Nasser overthrew Naguib in a bloodless coup and assumed control of Egyptian affairs, quickly becoming the country's dictator. Within a few years, Nasser had become the undisputed idol of the Arab Middle East and the voice of Arab nationalism. This left him vulnerable to the sentiments of the Arab Street and unable to pursue policies, such as peace with Israel, that were antithetical to

the faceless masses or to those who could protest loudest. He could have easily won an election, but Nasser did not have a particular attachment to Western institutions, as would be the case with his successors. Throughout his life, he sought to maintain the popularity he enjoyed with Egyptians, and later with Arabs in general, but without a mandate from the electorate he was hostage to the ebb and flow of public opinion. According to Tyler (2009):

> He (Nasser) had not invented Arab nationalism, but in the cauldron of postwar politics, out of the detritus of empire, it had invented him, and his clarion call was soon pulsating on Radio Cairo and the medium that radiated to ever corner of the region as the "Voice of the Arabs."
>
> (Tyler, 2009, p. 38)

Ironically, as Tyler (2009) further elaborates, the CIA had provided Nasser with a transmitter powerful enough to reach every town and village in the Middle East.

Not since the fall of the Ottoman Empire had an individual come close to representing the moral authority that had rested with the sultan-caliph. Unlike Ottoman potentates, however, Nasser was a secular leader who sought to charter a course towards modernity for the Arabs and the Middle East. Ideologically, Nasser was pro-American and anti-communist, but as Aburish (2005) states, "his admiration for America did not limit or diminish him. Unlike other Arab leaders of his time and later, he did not depend on America to exist" (p. 144). Perhaps because of this, and because of his empathy for the people of the region, he was able to transcend from Egyptian strongman to Arab icon. In this context, although he was initially in favor of peace with Israel, he had to respond to the wishes of the Arab masses the demonstrators who claimed to represent them who could not accept Israel; as the ultimate Palestinian victory had become the *idée fixe* with most Arab and Muslim intellectuals and radicals. In this context, Nasser had the knack of knowing when to lead the Arab world and when to follow it, but the situation made it difficult for him to secure the confidence of the Americans. Equally problematic for Nasser were the humiliating Israeli raids into Egypt that made it impossible for him to negotiate from a position of weakness with respect to Israel, which, in turn, made it difficult for any US administration to back overtly the Egyptian dictator.[31]

As long as Nasser could not reach an accommodation with Israel, the US could not openly support him or, more significantly for Nasser, provide him with substantial modern weapons. Nasser, for his part, could not commit to American or British anti-Soviet organizations while the greatest threat to Egypt was Israel. He refused to join the British-sponsored Baghdad Pact, which was aimed as much at containing Soviet influence in the region as at countering Nasser's perceived ambitions.[32] Early in 1955, Tyler (2009) notes, Nasser appealed to the United States for weapons to defend Egypt's border from Israeli incursions. Indeed, the state of Egyptian military hardware was poor, lacking sufficient modern weapons. When Nasser's entreaties to Washington failed, he turned to the Soviet Union, which supplied him with anywhere from 90 to 200 million

dollars' worth of equipment. This amount was substantially more than the 27 million Nasser had requested from the Americans. Earlier in April 1955, he had attended the Bandung Conference in Indonesia and joined with Jawaharlal Nehru and Zhou Enlai in the formation of the Non-Aligned Movement. On 16 May 1956, Nasser recognized Mainland China, and Smith (2012) explains that this proved to be too much for many in Congress and in the US Departments of State and Defense, as well as in the intelligence community, who became convinced that the Egyptian dictator was now in the enemy camp. Smith (2012) elaborates that although Eisenhower was less inclined to abandon Nasser, John Foster Dulles, who was left in charge of America's foreign policy after the president was incapacitated with ileitis, used the opportunity to scuttle American support for the construction of the Aswan Dam. Nasser had been prepared for the rejection and had already secured Soviet financial support for the project.

This terminated the American relationship with Nasser and by extension the prospect of an Arab–Israeli settlement that could have contributed to the stabilization of the Middle East. Dulles's anti-communism and the influence of Israel's supporters in Congress won the day, but it was a shortsighted victory. Nasser was the only Arab leader who had the credibility and mass appeal to bring about a rapprochement between Israel and the Arabs and by extension, with the Muslim world. The difficulty was that the Americans did not understand the Middle East context. Nasser needed a great deal of time to cement his influence in the region so that with respect to Israel he could lead and not follow. The Americans could not or would not understand that an effective Arab leader could not be, or be seen to be, beholden to any foreign power.

Although the US condemned the 1956 Anglo-French invasion of the Canal Zone, the Suez Crisis further enhanced Nasser's stature in the Arab world, and it did little to ameliorate the conviction that the Islam world was under constant threat by the West. Nasser was seen as the symbol of independence and a bulwark against the incursions of the Europeans and even the Americans, despite the actions of the White House over Suez. Even the 1967 war, in which Egypt and the Arabs suffered a humiliating defeat, only served to underscore suspicion of the West and practically made Nasser a hero—to many in the region a victim of Israeli and American aggression. The ultimate irony, of course, was that Nasser was the only Arab leader who could contain the influence of Muslim fundamentalists and extremists such as the Muslim Brotherhood.

After the US Government severed all links to Nasser in 1956, the CIA continued to expand its ties with former Soviet Muslims who had served in the German Army during the Second World War. Part of the Truman and later the Eisenhower administration's policy of containment was to conduct covert operations against the Soviets, which included collaboration with radical Muslim organizations who opposed communism. To this end, in 1951 the US established the American Committee for Liberation, which operated Radio Liberty and recruited for the most part, Muslims who could be used to penetrate the Soviet Union. In the 1950s, the population of the USSR included over 30 million Muslims, some of whom could be reached by their émigré relatives—at least

that was the conviction in the CIA. The émigrés were mostly ex-Waffen SS recruited by the Nazis from Soviet prisoners of war and convinced to fight against the Red Army. Although many of these were repatriated to the Soviet Union, Johnson (2010) explains that the US authorities found better use for those who escaped and ensured that they, and many others in the displaced person camps in Germany, became sources of recruits in the covert struggle against communism.[33]

Political Islam and terrorism

After the mid-1960s the CIA and the Muslims drifted apart—the Vietnam War distracted the CIA, and relations with ex-Soviet Muslim and radical Muslim organizations went dormant. The Iranian Revolution in 1979 and the emergence of the Ayatollah Khomeini's rabid anti-Americanism, however, reverberated throughout the Shia as well as the Sunni communities around the world and helped to inspire a new generation of Islamic militants. The anti-Americanism in the Muslim world was not affected by the previous relationship between the Muslim Brotherhood and the CIA because this relationship had remained secret. The most visible aspect of America's policy in the Middle East, consequently, was how successive US administrations lent their unqualified support to the state of Israel. This fed the conspiracy theories in the Muslim world regarding the US and Israel.

One such instance was the 1979 incident that took place in the Great Mosque of Mecca.[34] On 20 November of that year, just before the beginning of the Islamic New Year, approximately 200 well-armed militants (including women and children), led by Juhaiman al-Utaibi and Abdullah al-Qahtani, seized the Al-Masjid al-Haram mosque in Mecca. Utaibi came from a prominent Arab family; he and the other militants were members of the puritanical Wahhabi sect, the official state version of Islam in Saudi Arabia. Most of them had been students at the Islamic University of Medina. The group included locals as well as Muslims from other countries.

A certain number, as Al-Rasheed (2002) elaborates, were also members of the Egyptian Muslim Brotherhood. The presence of Muslim Brothers in Saudi Arabia was an example of regional blowback. King Faysal had invited the Muslim Brotherhood refugees to Arabia in the 1960s as part of a scheme to undermine Nasser, after the latter disbanded the Society and imprisoned or executed thousands of its members. Many Muslim Brother refugees accepted Faysal's asylum and became active in several of the new religious universities established by the Saudi royal family, through which they had come into contact with Juhaiman al-Utaibi and Abdullah al-Qahtan.

The capture of the Great Mosque was not only a religious act but also meant to stir up an Islamic uprising against the Saudi royal family. After he took over the mosque, Utaibi condemned the House of Saud for its moral laxity, corruption, and the destruction of Saudi culture by imitation of the West. According to him, the Saudi monarchy had lost its legitimacy and thus had to be removed. He

also proclaimed, as Wilson and Graham (1994) document, that Abdullah al-Qahtani was the true "Mahdi"[35] and asked the Imam leading the morning prayers to proclaim him as such.

The seizure of one of the most sacred mosques in Islam stunned Muslims throughout the world and had considerable repercussions for the United States and its allies. A flurry of rumors, conspiracy theories and outright fantasies carried the crisis in Mecca to just about every corner of the Muslim world. In Islamabad, a local newspaper proclaimed that an American task force in Arabia was landing in order to take control of the Persian Gulf. A short while later, the same newspaper revealed that Israeli paratroopers were to be dropped on Mecca or Medina, perhaps both. The theocratic regime in Tehran immediately stated:

> It is not far-fetched to assume that this act has been perpetrated by the criminal American imperialism so that it can infiltrate the solid ranks of Muslims by such intrigues. It would not be far-fetched to assume that, as it has often indicated, Zionism intends to make the House of God vulnerable.
>
> (Trofimov, 2007, p. 275)[36]

The capture of the mosque made few headlines in the West and was quickly overshadowed by the Soviet invasion of Afghanistan. The conspiracy theory that the mosque was seized by Israeli and US forces, especially after the Ayatollah Khomeini pronounced it as fact, assumed a life of its own and triggered violent demonstrations.

On 21 November, the day after the Grand Mosque was seized, Pakistani students and militants from Pakistan's militant Islamic organizations stormed the American embassy in Islamabad and burned down the building while Pakistani police and security forces slowly came to the rescue of the Americans. The howling mobs were driven by the conviction that the United States had seized the Grand Mosque and they had to exact vengeance. Although a major Kuwaiti Newspaper, *Al Siyassa*, published long extracts of the musings of the rebels in the Grand Mosque on 29 November, many Muslims continued to assume that the capture of the mosque was the work of a variety of hostile foreigners. Mobs of young militant Muslims and students attacked American institutions in Turkey, India and Bangladesh and stormed the American Embassy in Tripoli, Libya.[37]

The retaking of the Grand Mosque was accomplished by Saudi troops under the direction of a French anti-terrorist unit.[38] Officers from the Groupe d'Intervention de la Gendarmerie Nationale were brought to Mecca two weeks later and trained a select number of Saudi military. Under distant French supervision, notes Trofimov (2007), the Saudis hunted down the militants by flooding the basement of the mosque and its tunnels with the chemical dichlorobenzylidene-malononitrile—an irritant that blocks respiration and is non-lethal as long as the subject of the attack is removed in less than five minutes. The operation was successful and a large number of the insurgents were captured. Sixty-three survivors were publicly beheaded on 9 January 1980.

For most of the outside world, the incident at the Great Mosque was a solitary act: yet another episode in a series of confrontations between radicals and state authority in the tumultuous Middle East. The rebels who challenged the legitimacy of the Saudi dynasty, however, highlighted the rise of a more aggressive militant Sunni Islam in its various manifestation throughout the Muslim world. In 1979–80, however, the West and many of the conservative Middle Eastern governments were too concerned with Khomeini's brand of Shiite Islam to note this development. Indeed, the United States was beginning to tap into the militant stream of Wahhabism in order to secure Islamic *mujahidin* (Islamic freedom fighters) for the covert war against the Soviets in Afghanistan. The Saudis, as well as other Middle East governments, anxious to rid themselves of potential troublemakers and to be of assistance to the Americans, killed two birds with one stone by facilitating the transportation of these new covert warriors to the Islamic jihad in Afghanistan.[39] In that unfortunate country, the *mujahidin*, under the guidance of experts from the CIA working through Pakistan's Inter-Service Intelligence Agency, acquired the tradecraft of espionage, sabotage, commando tactics, psychological warfare and counterintelligence, which later they successfully employed against the West.[40] The use of suicide through martyrdom was an added innovation that separated Muslim terrorists from similar fanatics in the West.

Conclusion

The Soviet invasion and occupation of Afghanistan followed by the American invasion and occupation of Afghanistan and Iraq a few decades later were for many Muslims a continuation of European colonialism and oppression. Colonialism, writes Dawisha (2003), was subsumed by imperialism and became the much needed "other" for Arab nationalism. This was particularly the case at the height of Arab nationalism between 1954 and 1967, personified by Nasser. The ideological construct of anti-imperialism was based on the notion that Dawisha (2003) describes: "The 'imperialist forces' were outsiders, alien to the area, had committed many injustices against the Arab people, and therefore were 'deserving' of the abuse heaped upon them" (p. 28). When Nasser's brand of nationalism and socialism collapsed after his death, corruption and poverty became endemic in Egypt. Other Middle Eastern societies followed, which served to underscore the failure of Arab nationalism and, along with it, secularism. For the Arabs, as well as the other Muslims, secular leadership and secular states became synonymous with failure and systemic corruption.

Historic injustice perpetrated by the West is one of the themes employed by terrorist groups to secure recruits and justify acts of violence against the United States and its allies, in and outside the Middle East. Another theme has been the notion that returning to what the terrorists imagine were the precepts of Islam in the time of Muhammad will cure all the ills that plague the Muslim world. Finally, for militants and jihadists, and for a considerable number of young Muslims, European colonialism has been replaced by American imperialism,

which, in turn, is linked to the US alliance with Israel. The on-and-off violence between the Israelis and Palestinians and the US occupation of Afghanistan and, until recently, Iraq, are reminders that that there are still regions under the control of the West and its allies. All these themes, combined with the suicide bombers and the deaths resulting from drone attacks, provide a source of martyrs that confer legitimacy on the ongoing holy war. Martyrdom is the ultimate mechanism that not only underscores the ongoing jihad but is also compelling evidence for potential recruits of the theological justification for suicide.

Other evidence is provided by military success as demonstrated by the Islamic State of Iraq and Syria (ISIS), now the Islamic State (IS). This offshoot of Al-Qaeda includes not only Muslim extremists but also disgruntled Sunni Muslims from Iraq and Syria, along with Baathist civil servants, soldiers and officers dismissed by the Americans in 2003 and later by Baghdad's Shiite government. Armed with US military hardware, which they seized from the Iraqi army, IS has emerged as a formidable terrorist organization and military force. The jihadists have conquered large tracks of Syrian and Iraqi territory, which has given them possession of petroleum resources that afford them the wealth with which to carry on their conventional battles in the region and future terrorist acts against the West.[41] Unlike the Muslim Brotherhood, Hezbollah, Hamas and Al-Qaeda, which killed civilians in bombings but did not deliberately kill innocent bystanders that were trapped in a targeted area, the followers of the Islamic State relish mass executions, torture, rape and wanton destruction. The Islamic State imposes a puritanical Wahhabi version of Islam that even the adherents of Al-Qaeda cannot stomach and is consciously trying to ignite a religious war between Sunnis and Shia as well as between Muslims and Christians.

An intriguing consideration is that the Islamic State is the manifestation of an evolutionary political and religious process initiated by the Muslim Brotherhood, accelerated by Al-Qaeda and culminating in the so-called caliphate proclaimed by al-Baghdadi, the shadowy leader and caliph of the Islamic State. Unlike Osama bin Laden, Abu Bakr al-Baghdadi maintains a very low profile and rarely meets the media or issues public pronouncements. Furthermore, in contrast to bin Laden, he did not use terror to inspire a mass uprising of Muslims to reestablish a future caliphate. Rather he assumed the title of caliph regardless of Islamic law and tradition. Under his direction the Islamic State is using terror as the spear-point to expand the caliphate and reclaim Sunni territory as well as force the conversion of unbelievers, including Shia, to the "true faith." Indeed, its main export will be to send indoctrinated young men and women to their countries of origin programmed to spread death and destruction.

Notes

1 Part of this study drew inspiration and some modified content from the author's monograph: Gerolymatos (2010).
2 Spies or combatants out of uniform have few or no rights and, depending on the country, are often executed or tortured with impunity.

3 Shiite Muslims, however, did not acknowledge a Sunni caliph. Indeed, the succession issue with respect to the caliphate is at the heart of the Shiite–Sunni schism. See Nasr (2006, pp. 40–43).
4 Hagen (2004) points out that in addition to Sharif Hussein's claims on the caliphate, Abbas Himli, the Khedive of Egypt, attempted to have himself proclaimed caliph before the outbreak of the First World War.
5 The Bolsheviks published the Sykes–Picot Agreement in *Izvestia* and *Pravda* on 23 November 1917. Three days later, on 26 November, the *Manchester Guardian* published it in English.
6 On these debates, see Karsh (2006, pp. 127–130).
7 Regardless of the small number of activists in the Arab secret societies, those Arabs who joined the British in the war assumed they would be able to take part in the debates over the future of the Middle East, and a few had the opportunity of gaining experience in government within the British Mandate administrations. See Dawisha (2003, p. 41).
8 In the 1920s the Khilafat Movement sprang up throughout the British colonial territories in Asia to defend the Ottoman caliphate. It was particularly effective in British India, where it formed a rallying point for Indian Muslims and was one of the many anti-British political movements to secure widespread support. For a few years it worked in alliance with Hindu communities and was supported by Ghandi, who was a member of the Central Khilafat Committee. The movement came to an end in 1924, after the British incarcerated most of the leadership, and several parts broke off to establish their own organizations. See Rahnema (2005, pp. 100–102).
9 There is no evidence, however, that any of the Muslim or non-Muslim terrorist groups in the Middle East acquired their "tradecraft" from the successful use of terrorist tactics employed by the Irish Republican Army (IRA). The IRA adopted assassination, bombing, kidnapping and fear in order to wage war against conventional forces. In the case of the IRA, religion was also a factor. In 1920–21, when the IRA struggle against British police and military spread to Northern Ireland, it turned into a sectarian conflict between the majority Protestants against the minority Catholics in the six counties of this part of Ireland. In the second round of the IRA campaign in Northern Ireland, the religious factor ensured that sectarian violence practically overshadowed the political agenda of the Irish nationalists. For the earlier Irish war see Townshend (2013); on the outbreak of hostilities in Belfast and the resumption of IRA activities see Coogan (2000). On the other hand, the IRA's tactics influenced European terrorist and radical organizations such as the German group Revolutionäre Zellen.
10 Al-Banna founded the Muslim Brotherhood in the city of Ismailia with six workers from the Suez Canal Company.
11 Egyptian pounds.
12 On one occasion, Western and Middle Eastern radicals even collaborated on a joint operation. On 27 June 1976, two Palestinians from the Popular Front for the Liberation of Palestine, External Operations (PFLP-EO) hijacked Air France Flight 139 with two Germans, Willfred Böse and Brigette Kuhlmann, of the group Revolutionäre Zellen.
13 Morris (2008) argues that the outbreaks of 1920, 1929 and 1936–39 grew progressively more lethal and extensive.
14 In the 1960s and 70s, when many Afghan religious scholars came under the influence of the Muslim Brotherhood, Qutb's ideas attracted particular interest at the faculty of religious law in Kabul, and the scholar Burhanuddin Rabbani translated his writings into the Dari Afghan language.
15 In 1954 a would-be assassin fired several shots at Nasser, who was giving a speech, but missed.

16 The group was organized by Reinhard Gehlan, a former German army general in charge of the German armed forces' eastern front political and field intelligence organization, Fremde Heere Ost (Foreign Armies East), which had focused on gathering intelligence and mounting covert operations against the Soviet Union during the Second World War. Towards the end of the war, Gehlen hid his files on the Soviet Union and offered his services to the Americans. The group eventually came under the control of the CIA.
17 Cairo Embassy to African Department, 6 February 1953, V6703174, FO 371/102869, TNA.
18 While some of the German specialists were, like Fahrmbachers, essentially military men, there was also a core of considerably less reputable ex-Nazis including a cross-section of former SS, Waffen-SS, Gestapo, and Sicherheitsdienst (SS Security Service); virulently anti-Semitic propagandists from Goebbels' information ministry; and former medical officers, administrators and guards from the death camps of the Holocaust, who were purposely recruited to construct and run desert concentration camps for Nasser.
19 Some of the war criminals included SS Major-General Hermann Lauterbacher, Gauleiter of Hannover and former deputy leader of the Hitler Youth, who was tried for war crimes and discharged on a technicality, sent by Gehlen to Egypt as BND liaison officer; Professor Johannes von Leers, vicious anti-Semite and senior official in Goebbel's propaganda ministry, said to have been recommended by Amin al-Husseini, the former Mufti of Jerusalem, whom he knew well in Berlin; his close associate, SS Lieutenant Franz Bünsch, best known for his pornographic work, co-authored with Adolf Eichmann, *The Sexual Habits of the Jews*, who also had served in Eichmann's Jewish Affairs section at the Reichssicherheitshauptamt (SS headquarters) and who proposed setting up for Nasser a grandiose global intelligence network staffed by Egyptians and ex-Nazis from all over the world; and SS Colonel Sepp Tiefenbacher, Himmler's personal chief of security and friend of the al-Husseini. See CIA Name Files Issue 1: 32–2000/06/07 and Issue 2: 45–2002/A/11/2, RG263, NARA (Lauterbacher); Issue 1: 32–2000/06/07, RG263, NARA (Leers); Issue 1: 51–2000/07/04 and Issue 2: 52–2002/A/11/3 RG263, NARA (Tiefenbacher). For more about Bünsch, see Copeland (1969).
20 "Egyptian soldiers learn the German way" (1953), *Daily Telegraph*, 17 July, JE1202/16, FO 371/102869, TNA.
21 Hankey to Salisbury, 20 July 1953, JE1202/15, FO 371/102869, TNA.
22 Ibid.
23 "Egyptian Para-Military Forces," HQBTE Report, August 1953, JE1202/24, FO 371/102869, TNA.
24 HQBTE Report, May 1953, JE1202/15, FO 371/102869, TNA.
25 Ibid.
26 "Egyptian Para-Military Forces," HQBTE Report, August 1953, JE1202/24, FO 371/102869, TNA.
27 HQBTE Report, May 1953, JE1202/15, FO 371/102869, TNA. 9 BAD was the 9th Base Ammunition Depot, Royal Army Ordinance Corps, which was permanently situated near the village of Abu Sultan.
28 "Egyptian Para-Military Forces," HQBTE Report, August 1953, JE1202/24, FO 371/102869, TNA.
29 Ibid.
30 Ibid.
31 On 28 February 1955, the Israelis attacked the Egyptian military headquarters in Gaza, blew up the building and killed 38 Egyptian soldiers. Israeli covert operations also exposed Egypt's vulnerability and undermined Nasser. See Aburish (2005, p. 226).
32 The Baghdad Pact was a defensive organization for promoting shared political, military and economic initiatives founded on 24 February 1955 by Turkey, Iraq, Great Britain, Pakistan and Iran. Similarly to the North Atlantic Treaty Organization and the Southeast Asia Treaty Organization, the main purpose of the Baghdad Pact was to

prevent communist incursions and foster peace in the Middle East. It was renamed the Central Treaty Organization, or CENTO, in 1959 after Iraq pulled out of the Pact. It was dissolved in 1979.

33 An account of the recruitment of former Soviet Muslims and links between the CIA and the Muslim Brotherhood in the 1950s and afterwards is ably provided by Johnson (2010).

34 The Great Mosque is one of the most sacred locations for pilgrims to the annual Hajj and can accommodate close to 300,000 people. At the center of its courtyard, which is 40 acres in size, is the Kaba, a cube-shaped structure always covered by a black cloth embroidered in gold. Muslims believe that Abraham built this to honor God and that Muhammad in 630 BCE cleansed it of idols. Over 2,000,000 pilgrims each year conduct their prayers and rituals at this site.

35 The Mahdi is the Islamic messiah who is supposed to appear at the end of the new century (in this case the twenty-first century).

36 "Khomeini in Mecca Attack," *FBIS Middle East Report*, 21 November 1979, cited in Trofimov (2007), p. 275.

37 One hundred and thirty-seven American diplomats and marines were trapped in the embassy. Two marines were killed, as were an American pilot and two Pakistani embassy staff.

38 The question on whether to use force was submitted to the Ulema (the religious establishment), which after some deliberation sanctioned the use of government troops to remove the militants from the mosque. According to Wilson and Graham (1994, p. 58), the Ulema took a day-and-a-half to formulate a judgment. One report in *Time* magazine claimed it took the Ulema eight hours, while a second report filed one week later stated that the ruling was issued on the third day of the siege: *Time* (1979); Brellis (1979).

39 Although some writers, like Cooley (2000, pp. 83, 85–86, 195, 204), have claimed there have been assertions that the CIA, with or without other agencies of the US government, directly trained Arab *mujahidin*, including Osama bin Laden, there is little evidence to support this, according to Bergen (2001, pp. 64–67). Instead, America's contact with Arab *mujahidin* was indirect. US aid in the form of training, weapons, and funding was funneled through Pakistan's Inter-Service Intelligence.

40 Saudi Arabia agreed to match US funding for the *mujahidin*, and Egypt permitted the US Air Force to use Egypt as a base from which it shipped to Pakistan tons of weapons and equipment. Even the Chinese contributed $600 million to the cause. Furthermore, the government of Anwar Sadat (Nasser's successor) trained volunteers from the Muslim Brotherhood for the jihad in Afghanistan. In the first years, in order to avoid any links with the US, the CIA secured weapons from the First and Second World Wars, stockpiled in countries such as Egypt, India and China. By 1985, 60,000 tons of equipment had been made available in Pakistan. See Prados (2006, pp. 471–472, 488) and Dreyfuss (2005, pp. 274–275).

41 Fresh conquests include the cities of Mosul and Fallujah and about one-third of Iraq.

References

Abbas, S. (2014) *At Freedom's Limit: Islam and the Postcolonial Predicament*. New York: Fordham University Press.

Aburish, S. K. (2005) *Nasser: The Last Arab.* New York: Thomas Dunne Books.

Al-Rasheed, M. (2002) *A History of Saudi Arabia.* Cambridge: Cambridge University Press.

Antonius, G. (2001) *The Arab Awakening: The Story of the Arab National Movement.* Safety Harbor FL: Simon.

Bergen, P. L. (2001) *Holy War, Inc.: Inside the Secret World of Osama bin Laden.* New York: Free Press.

Brellis, D. (1979) Struggle for the sacred mosque: Eight days in Mecca that shook the Muslim world. *Time*. *10* December, p. 48. Academic Search Premier, EBSCOhost. Accessed 24 September 2014.

Cairo Embassy to African Department (1953) 6 February. V6703174, FO 371/102869, TNA.

Coogan, T. P. (2000) *The IRA*. New York: Palgrave.

Cooley, J. K. (2000) *Unholy Wars: Afghanistan, America and International Terrorism*. Sterling, Pluto.

Copeland, M. (1969) *The Game of Nations*. New York: Simon and Schuster.

Dawisha, A. (2003) *Arab Nationalism in the Twentieth Century: From Triumph to Despair*. Princeton: Princeton University Press.

Dreyfuss, R. (2005) *Devil's Game: How the United States Helped Unleash Fundamentalist Islam.* New York: Metropolitan.

Egyptian Para-Military Forces (1953) HQBTE Report, August, JE1202/24, FO 371/102869, TNA.

Egyptian soldiers learn the German way (1953) *Daily Telegraph*, 17 July. JE10202/16, FO 371/102869, TNA.

Esposito, J. (ed.) (2003) *The Oxford Dictionary of Islam*. New York: Oxford University Press.

Gerolymatos, A. (2010) *Castles Made of Sand: A Century of Anglo-American Espionage and Intervention in the Middle East.* New York: Thomas Dunne Books.

Hagen, G. (2004) German heralds of holy war: Orientalists and applied oriental studies. *Comparative Studies of South Asia, Africa, and the Middle East*. 24 (2), pp. 145–162.

Hankey to Salisbury (1953) 20 July. JE1202/15, FO 371/102869, TNA.

Harris, C. P. (1964) *Nationalism and Revolution in Egypt: The Role of the Muslim Brotherhood.* The Hague: Mouton.

HQBTE Report (1953) JE1202/15, FO 371/102869, TNA.

Hourani, A. (1962) *Arabic Thought in the Liberal Age, 1798–1939*. London: Oxford University Press.

Irwin, R. (2001) Is this the man who inspired Bin Laden? *Guardian*, 1 November. Available at: www.theguardian.com/world/2001/nov/01/afghanistan.terrorism3. Accessed 24 September 2014.

Johnson, I. (2010) *A Mosque in Munich: Nazis, the CIA, and the Rise of the Muslim Brotherhood in the West*. New York: Mariner Books.

Karsh, E. (2006) *Islamic Imperialism: A History*. New Haven: Yale University Press.

Lia, B. (1998) *The Society of the Muslim Brothers in Egypt: The Rise of an Islamic Mass Movement, 1928–1942*. Reading: Ithaca.

Lüdke, T. (2005) *Jihad Made in Germany: Ottoman and German Propaganda and Intelligence Operations in the First World War.* Münster: LIT.

Mango, A. (2010) *Ataturk: The Biography of the Founder of Modern Turkey*. New York: The Overlook.

Mitchell, R. P. (1969) *The Society of the Muslim Brothers*. New York: Oxford University Press.

Morris, B. (2008) *1948: A History of the First Arab–Israeli War*. New Haven: Yale University Press.

Naftali, T. (2005) Reinhard Gehlen and the United States. In Breitman, R., *et al.* (eds) *U.S. Intelligence and the Nazis*. Cambridge: Cambridge University Press, pp. 375–419.

Nasr, V. (2006) *The Shia Revival: How Conflicts within Islam Will Shape the Future.* New York: Norton.

Peters, R. (1979) *Islam and Colonialism: The Doctrine of Jihad in Modern History.* The Hague: Mouton.

Pipes, D. (1996) *The Hidden Hand: Middle East Fears of Conspiracy*. New York: St. Martin's Press.

Prados, J. (2006) *Safe for Democracy: The Secret Wars of the CIA.* Chicago: Ivan R. Dee.

Rahnema, A. (2005) *Pioneers of Islamic Revival*. London: Zed.

Smith, J. E. (2012) *Eisenhower in War and Peace*. New York: Random House.

Time (1979) "Sacrilege In Mecca Agony and hysteria as zealots seize the Sacred Mosque." 3 December, p. 50. Academic Search Premier, EBSCOhost. Accessed 24 September 2014.

Townshend, C. (2013) *The Republic: The Fight for Irish Independence, 1919–1923.* London: Penguin Books.

Trofimov, Y. (2007) *The Siege of Mecca: The Forgotten Uprising in Islam's Holiest Shrine and the Birth of Al-Qaeda.* Doubleday.

Tyler, P. (2009) *A World of Trouble: The White House and the Middle East—from the Cold War to the War on Terror.* New York: Farrar Straus Girroux.

Wilson, P. W. and Graham, D. F. (1994) *Saudi Arabia: The Coming Storm.* New York: M. E. Sharpe.

3 The gray cygnet problem in terrorism research

Laura Huey, Joseph Varanese and Ryan Broll

Introduction

In early April 2013, something strange happened. CBC News, Canada's public broadcaster, released a story identifying two Canadian youth involved in a deadly terrorist attack on an Algerian gas plant. Following the January attack, Algerian sources claimed Canadian jihadists had been involved; however, it was not until March—when Royal Canadian Mounted Police (RCMP) officers were sent to Algiers to investigate—that the nationality of the two dead attackers was officially confirmed. Citing unnamed sources, CBC News subsequently identified the young men and the story was quickly picked up by other national and international media outlets. This strange tale was fueled further when two other young Canadian males, both of whom were friends with the dead jihadists, were identified as having suspected links to Al-Qaeda.

The radicalization of Western youth is no longer a surprising phenomenon. Even the most cursory of Internet searches reveals several hundred books, book chapters, articles and commentaries on the rise of radical Islam and the ability of its proponents to convert European, Australian, American and Canadian citizens into "homegrown terrorists" who operate in their home country and abroad. The predominant focus of much of this literature is also not surprising: the majority of studies examine first- and second-generation Muslim males, or those termed "1.5s."[1] And perhaps this focus is just, since it is these young men who are frequently cited as actors in numerous jihadist-inspired movements (Bakker, 2006; Silber and Bhatt, 2007; Jenkins, 2011). Thus it was not particularly surprising to learn that two of the young Canadians linked to terrorist activities were Muslim males from immigrant families: Ali Medlej was Lebanese and Mujahid Enderi was Libyan. Instead, it was the involvement of the two other second-generation youth that occasioned surprise: Xristos Katsiroubas (Greek) and Aaron Yoon (Korean).

Katsiroubas was one of those killed during the siege of the Algerian gas plant. Once his name and that of Medlej were released, news reporters quickly linked both men to Yoon, who had been quietly arrested in 2011 in Mauritania as a member of Al-Qaeda (MacCharles, 2013). Another high school friend of Katsiroubas and Medlej, Enderi is believed to have ties to Al-Qaeda and remains

at large (Brewster *et al*., 2013). It is unclear how these young men came to adopt radical Islamic ideologies. While Medlej and Enderi were practicing Muslims, Katsiroubas came from a Greek Orthodox family and Yoon converted from Catholicism (Humphreys *et al*., 2013); thus the latter two men had no previous cultural or social ties to Islam. This fact, along with their cultural backgrounds, engendered much local surprise when news of their conversion to radical Islam broke. And yet, this surprise was not wholly warranted for two reasons. First, it was hardly the first time that Western media had reported the presence of non-Muslim names among those identified as Western converts to radical Islam. The cases of Richard Reid, John Phillip Walker Lindh, Thomas Fischer, Samantha Lethwaite, Germaine Lindsay, Christian Ganczarski and Steven Smyrek illustrate this point. What differentiated Katsiroubas and Yoon from Lindh and Reid, among others with whom their cases are often indiscriminately lumped together as "non-Muslim converts" to terrorism, was that the former were, like Enderi and Medlej, children of immigrants and thus were, in some ways, likely to have encountered the experiences of cultural tensions and divides frequently reported by the offspring of immigrant parents. In essence, then, Katsiroubas and Yoon were, at once, both like and not like other Western terrorism converts. That said, their situation was not wholly unprecedented. José Padilla, born in New York of Puerto Rican immigrant parents, was convicted for his role in planning bombing attacks against US targets. Indeed, the Katsiroubas and Yoon cases are not even the first time that the name of a second-generation convert appeared on a list of suspected Canadian jihadists. In 2006, Steven Vikash Chand, who had been raised by Hindu Fijian parents, was arrested and later convicted for his participation in a set of jihadist plots known as the "Toronto 18" case (Silber, 2011).

It is the nature of social scientists to want to explain, and thus to predict, human behavior. This is no less true of terrorism researchers. Even so, the curious case of Chand—which now occurred almost a decade ago—has produced not so much as a tiny ripple in the sea of terrorism studies. Using an academic search engine (Summon), we located only one reference to Chand in a book (see Williams, 2007); Google Scholar identified one additional mention in a New York Police Department report (see Silber and Bhatt, 2007). Within this chapter, we wish to explore this lack of interest in Chand and others like him—Padilla and Lindsay being two other and slightly better known examples—and examine what it tells us about the direction of contemporary terrorism studies and the need to re-evaluate how we study domestic radicalization. To do so, we will first discuss current themes in the literature on domestic radicalization, before we invoke what we refer to as the "gray cygnet," a variant of Nassim Taleb's (2007) concept of the "black swan" event. In essence, we argue that the Chand case and others like it—such as the more recent stories of Katsiroubas and Yoon—represent anomalies within the terrorism field. In view of this, studying these cases would seem to hold little predictive value. However, even outliers, which these cases may be described as,[2] should be closely examined before being discarded as being irrelevant (Chatterjee and Hadi, 1986). Cases such as Chand's are important for understanding and testing the strength of

existing models of domestic radicalization among second-generation youth. Perhaps even more importantly, they are important for developing new, empirically sound lines of thought.

The radicalization of Westerners

Discussions of terrorism have been fraught with a number of conceptual and empirical problems. As a result, the terrorism literature has recently transitioned from defining terrorism in conceptual (and somewhat amorphous) terms toward identifying those factors that influence engagement in terrorist activities (Horgan, 2008). Radicalization—the process through which individuals (typically Westerners) become involved in terrorism (Lynch, 2013)—has a no less troubled academic history, having been described as a conceptually incomplete (Lynch, 2013; Richards, 2011) and problematic (Coppock and McGovern, 2014) term. Nevertheless, attempting to identify the antecedents of radicalization is at the forefront of terrorism research (Coppock and McGovern, 2014). Given that the study of radicalization is still in its infancy, several important questions remain unanswered. However, it is believed that only a minority of the many targeted for conversion to terrorism by terrorist leaders become radicalized, and even fewer ever engage in terrorist acts (Wilner and Dubouloz, 2011). Indeed,

> there is a difference … between solely accepting radical ideas and actively participating in violent behaviour as a result of one's views. Not all, and in fact potentially few, individuals who radicalize—even among those who vocally support violence in the name of their adopted cause—end up participating in violent behaviour.
>
> (Wilner and Dubouloz, 2011, p. 420; Horgan, 2005, 2008; Tessler and Robbins, 2007)

At the same time, as individuals become radicalized they simultaneously become more marginalized from conventional society and more integrated within their smaller extremist community (Horgan, 2008).

It is believed that those who become radicalized have some vulnerability to extremist messages. Since the terrorist attacks of 11 September 2001 in the USA (9/11) and the attack of 7 July 2005 on the London transport system (7/7), immigration has been a central feature of the political framing of radicalism and terrorism (Lynch, 2013). In particular, second- and third-generation (Muslim) immigrants are believed to be particularly susceptible to radicalization (Coppock and McGovern, 2014). Stroink (2007) argues that the Western-born children of immigrants are a valuable group for terrorists, with some of these youth being unusually receptive to violent ideals. Specifically, second-generation immigrants can be distinguished from others by their bicultural identity, which affords them in-group status with two cultures. This biculturalism has great strategic value for terrorists (Stroink, 2007).

Aside from a focus on immigration, there is little agreement about other factors that influence the conversion of Westerners to terrorism. Researchers have proposed two rather distinct models to explain how radicalization occurs (see Porter and Kebbell, 2011, for a review). The first model, often called the individual model, seeks to identify sociodemographic and psychological differences between terrorists and non-terrorists (Krueger, 2008; Post, Sprinzak and Denny, 2003; Volkan and Harris, 1995). Muslims and recent converts to Islam (Bakker, 2006; Silber and Bhatt, 2007), support for radical Islam (McCauley, 2012), and opposition to US foreign policy (McCauley, 2012; Tessler and Robbins, 2007) are positively correlated with radicalization. In their study of Australian homegrown terrorists, Porter and Kebbell (2011) concluded that those who become radicalized are "unremarkable" and "ordinary." In their study, the men who converted to terrorism were in their late twenties, married, had children, were employed, and were attached to their community. In other words, they were similar to other Australians. Notwithstanding such findings, it is clear that a single terrorist profile has yet to be found (Horgan, 2008; Porter and Kebbell, 2011). A report by the British House of Commons (2006) on the events of 7/7 exemplifies some of the problems of profiling terrorists. The report finds that, of the four individuals responsible for the attacks and linked to Al-Qaeda, three were second-generation British citizens born to Pakistani parents and one was a "1.5," an individual who had emigrated as a child from Jamaica with his parents. Some of the terrorists were well-educated, others were not. Some were poor, others were not. Some were highly integrated into British society, others were not. And some had extensive criminal histories, while others did not. In other words, it would have been rather difficult to predict that these individuals from diverse backgrounds would come together to commit such a deadly attack.

Given the apparent difficulties in identifying a single terrorist profile, some have suggested that the transition from non-terrorist to terrorist is a process that results from a sort-of-perfect storm of conditions (e.g., sense of global injustice, declining social control, group dynamics). These models, known as process models, suggest that individuals follow multiple pathways to terrorist organizations (Innes *et al*., 2007), or from "pre-radicalization" to "Jihadization" (Silber and Bhatt, 2007). Some process models combine individual characteristics with a set of conditions in attempting to identify would-be terrorists. For example, Silber and Bhatt's (2007) process model of radicalization notes that second- and third-generation Muslim men are at increased risk of radicalization.

Despite the empirical uncertainty as to variables that influence radicalization, contemporary terrorism public policy in the US, UK, Australia and Canada often seeks to address the social and individual factors that "cause" radicalization (Coppock and McGovern, 2014; Jackson, 2009, Kundnani, 2012; McCulloch and Pickering, 2009). Thus there is a clear policy emphasis on identifying future terrorists (McCulloch and Pickering, 2009) and preventing radicalization (Britain's Prevent and Channel programs; Jackson, 2009; Kundnani, 2012).

Black swans and gray swans

In his bestselling book *The Black Swan* (2007), Nassim Taleb uses the concept of the "black swan" to refer to a highly exceptional event that provokes significant change and/or social upheaval. As Taleb puts it, black swans are high-impact, low-probability events that are unanticipated because of inherent limitations in our ability to reason from observation and experience. The illustrative example of this phenomenon is the erroneous belief among earlier Europeans that all swans were white because non-white swans had never been spotted. The subsequent sighting of a black swan on the Australian continent demonstrates "the fragility of our knowledge" (Taleb, 2007, p. xxi). Taleb's black swan concept also demonstrates that building predictive models solely on what is "the norm" in a given area can be a problematic enterprise, because doing so assumes that conditions will always remain orderly and are not subject to randomness. Horgan's (2008) description of his encounter with a senior government official delivering a presentation on terrorist profiling is exemplary of this:

> A senior official protested to me, "Profiles are useful. Of course they are. The reason is … that your average suicide bomber is not going to be the middle-aged, white, father of three kids." The context of this comment, made in the United Kingdom, is that such a suicide bomber has not been encountered *yet* [emphasis added].
>
> (Horgan, 2008, p. 84)

This is hardly a novel insight, as evidenced by Sir Francis Bacon's well-known admonishment to "beware the fallacies into which undisciplined thinkers most easily fall. They are the real distorting prisms of human nature. Chief among them: Assuming more order than exists in chaotic nature." The human desire to "tame chance" (Hacking, 1990), leads to the third criterion for classifying a phenomenon a "black swan" event: the creation of *ex post facto* explanations of the event that attempt to render it both explainable and predictable.

Although it is recognized by many that modelling highly rare events is something of an exercise in futility (Greene, 2010), we can see the drive for *ex post facto* explanations most clearly in relation to one such event subsequently labelled a black swan: the 9/11 terrorist attacks. Following 9/11, numerous attempts were made to make sense of this event. Notably, one cluster of *post facto* analytic activity focused on the supposed failure of law enforcement agencies to identify and prevent the terrorists' plans. For example, one of the authors once attended a presentation by a former Homeland Security Advisor who suggested that if all data generated on every individual within the US were pooled—phone records, Immigration and Naturalization Service databases, address information, commercial records, and so on—US security intelligence agents would have been able to connect each of the terrorists and, thus, prevent the events of 9/11 (Huey, 2011). According to Taleb, correctly predicting the events of 9/11 would have been highly unlikely for one simple reason: the idea that

terrorists might highjack American airplanes, crash them into the World Trade Center and the Pentagon and target Washington DC was not then within anyone's realm of possibility. As Taleb (2007) puts it, "had the risk been reasonably conceivable on September 10, it would not have happened" (p. xxiii), as various steps would have been taken to prevent any such occurrences.

However, there are other unusual events that are said to better lend themselves to the possibility of prediction. These are what Taleb terms "gray swans." Drawing on Benoit Mandelbrot's work on non-linear chaos, Taleb argues that there are some highly unusual events that *can* be modelled because they are not outside our realm of possibility. Because these "gray swan" events are phenomena which are often not at the forefront of our thoughts, and thus not typically the stuff of planning and other predictive exercises, they frequently catch us by surprise. As examples, one might point to the Euro crisis in Spain or the cyberattack on South Korean banks.

Gray and black swans both refer to large-scale events. But what about smaller-scale events that generate a lesser impact? For the purposes of this chapter, we term such an event a "gray cygnet"—that is, a baby swan of the possibly predictable variety. Rissland and Xu (2011) use the term 'gray cygnet' to denote "a case that follows a Black Swan, is *highly* similar to it, is also exceptional in outcome, and continues to provoke havoc or change" (p. 258). Our use of the term is different. According to our conceptualization, a gray cygnet consists of four criteria: (1) it is a phenomenon that falls within the realm of possibility; (2) it presents as an anomalous event or a statistical outlier; (3) it is at present small in scale and has a relatively lesser degree of impact than a black or gray swan; and (4) it has emergent properties, particularly the ability to develop into a larger, more catastrophic phenomenon. In relation to terrorism studies, we might say that the gray cygnet is our Steven Chand, José Padilla or Germaine Lindsay scenarios (and, more recently in Canada, our Yoon and Katsiroubas cases).

It is not unreasonable to ask whether gray cygnet cases really merit our attention. If the norm among homegrown jihadists is a male whose family comes from a Muslim culture, should we even focus on converts from other cultures? We think so. To illustrate why such things might matter, we point to the work of Michelle Stroink (2007). Writing of attempts to shoehorn second-generation youth into existing explanatory frameworks, Stroink (2007) argues

> there are many factors that influence a group's or an individual's rise to terrorism, and each of these may be important also for understanding terrorism among second-generation immigrants. This population is unique, however, in several key ways. One of these unique characteristics is their capacity to identify with and experience the worldview benefits of two cultural ingroups. Therefore, the degree to which a second-generation individual identifies with each culture is a critical orienting question that has implications for the meaning of a terrorist act and the likely contributing factors.
>
> (Stroink, 2007, p. 298)

In the case of the individuals we are interested in—our gray cygnets—there is an added complication that needs to be accounted for: these are bicultural youth who chose to reject both their parents' cultures and the culture of their birth in favor of being adopted into a third subculture, indeed a countercultural group. It might turn out that their pathways into terrorism are exactly the same as those of their Muslim second-generation counterparts, but we cannot at present make such claims with any degree of certainty.

A cygnet emerges

Upon his arrest in 2006, the unique nature of Steven Chand's involvement in the Toronto 18 case appears to have occasioned little interest from scholars or members of the general public. In many respects, Chand appeared to be a model second-generation Canadian. Born in Canada to Hindu parents who emigrated from Fiji, he joined the Canadian military and served for almost four years (Silber, 2011). At some point during his time in the military, Chand converted to Islam. Although there has been some speculation that he turned to radical Islam following his parents' divorce (Silber, 2011), the circumstances surrounding his conversion remain unclear. In any case, he began attending a Toronto mosque led by a radical Imam, Aly Hindy (Blackwell and Bell, 2006). Sometime thereafter, he became a member of a group of 18 radicalized men, who became known as the Toronto 18. The group ran a jihadi recruitment and training camp in rural Ontario where Chand, drawing on his military background, allegedly became a trainer (Silber, 2011). The group devised several terrorist plots, including bombing selected sites such as the Canadian Security Intelligence Service (CSIS) offices in Toronto and Parliament in Ottawa and beheading the Prime Minister. However, before their plans could be carried out the 18 jihadists were arrested as a result of a CSIS/RCMP joint investigation. In 2010, Chand was convicted for activities related to his efforts to raise funds for the terrorist group.

We do not know why the anomalous nature of the Chand case failed to generate interest among researchers; however, the reason may be that his case is that of a gray cygnet and thus reflects our research biases. Chand's background made him an outlier both in relation to his Toronto 18 co-defendants and in light of the statistical norm for radicalized second-generation youth. Thus, with the exception of one other comparable case (José Padilla in the US), Chand represented something of an aberration at the time. And yet his individual case failed to pique much interest among either researchers or the general public. The result of this failure to consider the larger implications of Chand's conversion to radical Islam meant the loss of early opportunities to abstract from his situation and send warning signals about the potential for radicalization processes to influence second-generation youth from non-Muslim cultures. Indeed, it is fair to say that when Katsiroubas and Yoon emerged as a second pair of gray cygnets in Canada, the appearance of their clearly non-Muslim names among those of other confirmed or suspected terrorists should not, as previously noted, have been unexpected.

Methodological musings: all swans probably don't look alike in the dark

A number of methodological and theoretical developments in the literature on domestic radicalization are worthy of consideration. One specific area of concern relates to how we analyze this phenomenon. The methodological reality is that we have a fixed set of cases upon which to draw, and unlike, say, datasets that include the entire population of prison inmates in the United States, this number of cases is relative small. For example, Bjelopera (2013) draws upon a sample of 62, Jenkins' (2011) dataset includes 172 individuals, Kleinmann's (2012) includes 82, and Silber and Bhatt (2007) employ five case studies (no sample size was reported); Bakker (2006) has one of the largest datasets with a sample size of 242. As Horgan (2008) notes, overgeneralizations often result from small sample sizes. After all, it is difficult to generate statistically significant observations, and thus over-arching explanations for a set of behaviors, when dealing with a small sample size. And it is here that the gray cygnet problem raises its downy head. If the variable "Muslim convert" is the norm, then the variable "non-Muslim convert" is an outlier. Outliers are often handled in one of two ways: either they are excluded from analyses to avoid skewing one's results, or one's hypotheses or theories are redefined so that data from a larger range of individuals may be accounted for. In the latter case, rescuing one's outliers allows for a larger sample size at the expense of specificity.

To illustrate the use of this "clumping" technique, we note that in a study of 62 identified cases in the US, Bjelopera (2013) does not distinguish between radicalized first-, second- or third-generation Muslims and recent converts. Similarly, Gartenstein-Ross and Grossman (2009) do not distinguish between first- and second-generation individuals, nor do they distinguish between those from immigrant and non-immigrant families. More recently, Kleinmann (2012)—who uses Gartenstein-Ross and Grossman's data—also does not distinguish between second-generation Muslims and non-Muslims. Nevertheless, Kleinmann (2012) concludes that "radicalization is at least in part due to individual-level factors in 59 percent of converts as compared to only 10 percent of non-converts" (p. 290). To be fair, the use of such approaches for managing outliers is not unique to terrorism researchers. Zellner (2007) has similarly decried over-inclusive tendencies within economics: "In view of the potential importance of unusual and surprising data, it is troubling to see how often outlying observations are discarded without thought or averaged with usual observations by means of 'robust' techniques" (Zellner, 2007, p. 331). A second methodological problem to which the gray cygnet draws our attention is the fact that all too often studies on domestic radicalization construct or employ models based on less-than-ideal forms of data and data collection. There are typically four types of data upon which researchers stake their claims.

The first consists of piecemeal datasets or case studies constructed from open-source materials: court records, media reporting, online blogs and so on. For example, Gartenstein-Ross and Grossman's (2009) examination of the precursors

to radicalization draws upon material collected from blogs, court records and similar sources. Although they report using "a reasonably high evidence standard" in relation to their inclusion and exclusion criteria (Gartenstein-Ross and Grossman, 2009, p. 30), they do not provide specifics, making it difficult for others to judge the credibility of their sources. Likewise, Bjelopera (2013) relies on unsealed records from the Department of Justice and "open source reporting." While such data has its uses, particularly in a field in which primary samples are difficult to come by and random samples would surely not return enough converts to be of value, secondary data ought to be used cautiously, especially when findings based on such data are used to make concrete policy recommendations.

A second common data source is to simply use other researchers' datasets. Usually, these datasets come from studies in which other researchers pieced together materials from open sources. As an example, Kleinmann's (2012) study of convert and non-convert radical recruits is based on an analysis of material collected by Gartenstein-Ross and Grossman (2009). Although there is much value in making one's dataset available to other researchers—and doing so may minimize some methodological concerns—many of the original limitations noted above remain.

A third strategy is to draw loosely (i.e., unsystematically) from a variety of academic accounts, media stories and other secondary sources. Although Cottee (2011) reports that he draws on "Sageman's findings and observations" (p. 730) in constructing his subcultural model of radicalization, in support of his model he cites seemingly random examples not only from the work of Sageman (2004) but also from Bakker (2006) and other sources. The result is another untested theory of radicalization based on other people's readings of open-source materials.[3] What differentiates Cottee's efforts from those of Kleinmann is that the latter is somewhat more systematic in his approach to analyzing someone else's data.

The last commonly used method is to make inferences through analogy. Wilner and Dubouloz (2010) offer an example of this approach by using transformative learning theory to understand processes of domestic radicalization. These scholars are interested in "investigating and identifying the internal cognitive processes inherent to identity transformation" (Wilner and Dubouloz, 2010, p. 50) among homegrown terrorists. Rather than conducting clinical interviews with such individuals or administering surveys with validated measures in order to understand, for example, converts' cognitive functioning, the authors import data, concepts and ideas derived from research in the disparate fields of health sciences and adult learning. We are not convinced that adult learners and terrorists are sufficiently similar to draw such comparisons. Moreover, on the basis of this study we cannot conclude that we have an empirically informed understanding of the cognitive processes that lead to identity transformation, either among our tri-cultural cygnets—such as Yoon, Chand and Katsiroubas in Canada—or in relation to the development of homegrown terrorists more generally.

A third methodological and theoretical issue has to do with the level of analysis. There are generally three approaches to this issue (Sageman, 2008):

(1) study individuals and construct their personal biographies, (2) study group and inter-group dynamics, and (3) look for macro-level explanations within and across societies. The problem lies in the treatment of these approaches as mutually exclusive. Macro- and micro-level approaches are perhaps the most common in terrorism research h, but both have their shortcomings. Micro-level approaches (or what is referred to above as "individual models") tend to compare sociodemographic and psychological characteristics of non-terrorists and terrorists. However, as noted, a clear profile of "the terrorist" has yet to be found (Horgan, 2008; Porter and Kebbell, 2011). Macro-level explanations (or "process models") are generally concerned with broad structures and social processes; these have been critiqued for lacking explanatory clarity. As Horgan (2008) suggests, one must ask why, given the great number of youth raised in the same social conditions, so few become radicalized? In contrast, Sageman (2008) has argued for the study of social networks, rather than searching for entirely macro- or micro-explanations. However, to the extent that individual pathways can lead to the formation of groups and vice versa, and these individual pathways often have very different precursors, some shaped by societal influences and others through personal temperament or even by random chance, there is something to be said for adopting a holistic approach that operates at all three of these levels.

An exclusive focus on any one level of analysis risks creating artificial distinctions that unnecessarily truncate our ability to develop powerful insights into this phenomenon (not to mention that we place ourselves at risk of committing ecological or exception fallacies). In his study of whether terrorism is group behavior, Taylor (2010) explains that his research question is largely unanswerable because of the countless social processes that individuals engage in each day. Or, as Lichbach (1998, p. 403) explains, "individuals more or less purposefully make history, society, conditions, and rules, yet history, society, conditions and rules make individuals. We are both autonomous creatures, innovators, and prisoners." The contaminating influence of each level on the other suggests value in exploring multi-level hypotheses in future studies of the radicalization process.

How can we learn from cygnets?

It is becoming fairly common for those who study domestic radicalization to throw their hands in the air and declare that this process is a multi-causal phenomenon that defies easy explanations (Wilner and Dubouloz, 2010). While we do not disagree with such statements, we also do not believe that we should stop engaging in theory and research on the subject altogether and write off domestic radicalization as a giant, impenetrable black-swan-type process. A more moderate view might be to suggest that, at a minimum, we reexamine our tools and techniques.

Such a retooling requires three steps. First, we ought to begin treating seemingly unalike cases (individuals and groups) *as* unalike until we have empirical

proof that their similarities are more scientifically meaningful than their differences. Current efforts to develop terrorist profiles or identify the social processes that push or pull individuals into radicalization are not yielding definitive results. Instead, we might explore the processes that second-generation Muslim males go through as one phenomenon, the processes that shape second-generation converts as another, and the processes that impact non-recent immigrant converts as yet another, and we might similarly treat various 1.5s as distinct groups. To do so entails a second step: an increase in micro-level projects from which we can produce meaningful results that can be analyzed comparatively across project datasets, and thus permit general observations to be abstracted. The inclusion of micro-level analyses in studies of domestic radicalization—of both the "norms" and the "outliers"—will also provide opportunities to improve the quality of our data by forcing us to develop alternative sources beyond news releases and court transcripts. While terrorists can reasonably be considered hidden populations, and perhaps even more hidden than other well-studied populations, this fact should not prevent us from strengthening our research standards and collecting primary data whenever possible. The third step involves taking a more holistic perspective in our research focus, one in which there is recognition of the fact that individuals, groups and cultures do not work independently of each other. Dislocating nature from nurture in studies of radicalization ignores the vast body of evidence from psychologists that nature and nurture likely both influence us (Brofenbrenner, 1986) and that we are influenced by variables at multiple levels—e.g., biological, psychological, social, community, society, cultural, historical (Lerner, 1987).

Research on radicalization and terrorism is fixated on locating generalizable patterns and profiles based on suspect data, at the expense of studying unique cases such as our gray cygnets. In a field in which we all study outliers—in a survey of the general population, homegrown terrorists are surely outliers—we are suggesting that we should not ignore our own outliers when constructing our models. Embracing the diversity among those who become radicalized, drawing upon sound empirical samples, and taking a multi-level approach to our research, we believe, will enrich our field and deepen our knowledge of the radicalization process.

Notes

1 First-generation immigrants are those who immigrate to a country and become naturalized citizens or permanent residents. Second-generation immigrants are the children of first-generation immigrants; these children may be citizens of their home country by birth. In contrast, the term 1.5 is used to refer to those individuals who immigrated to a new country at a young age and thus spent their formative years in their new country's culture and educational system.

2 Wainer (1976) introduced the concept of the "fringelier" to refer to uncommon events that are more likely to occur than outliers. Fringeliers fall around three standard deviations from the mean and exert strong influence on estimates, but they are not as obvious as outliers because of their position in the distribution. Given our earlier

argument that cases such as Chand, Yoon and Katsiroubas may not be as rare as many believe, it is perhaps more accurate to refer to such cases as fringeliers. Nevertheless, we will use the more common and generic term "outliers" when referring to such cases.

3 We recognize that some might suggest we are also "cherry-picking" examples to make a point. However, we would counter that we are not building or testing an explanatory model; rather, we are presenting a methodological argument.

References

Bakker, E. (2006) *Jihadi Terrorists in Europe, their Characteristics and the Circumstances in which they Joined the Jihad: An Exploratory Study.* The Hague: Netherlands Institute of International Relations.

Bjelopera, J. (2013) *American Jihadist Terrorism: Combating A Complex Threat.* United States Congressional Research Service report 7–5700.

Blackwell, T. and Bell, S. (2006) "Not so sharp" guy allegedly sought to behead PM. *Edmonton Journal*, 7 June, p. A4.

Brewster, M., Levitz, S. and Jones, A. (2013) Mounties seek fourth London, Ont. man in possible connection to Algeria attack. *The Globe and Mail*. Available at: www.theglobeandmail.com/news/national/mounties-seek-fourth-london-ont-man-in-possible-connection-to-algeria-attack/article11167096/. Accessed 25 June 2013.

Brofenbrenner, U. (1986) Ecology of the family as a context for human development: Research perspectives. *Developmental Psychology.* 22 (6), pp. 723–742.

Chatterjee, S. and Hadi, A. S. (1986) Influential observations, high leverage points, and outliers in linear regression. *Statistical Science.* 1 (3), pp. 379–416.

Coppock, V. and McGovern, M. (2014) "Dangerous Minds"? Deconstructing counter-terrorism discourse, radicalization and the "psychological vulnerability" of Muslim children and young people in Britain. *Children and Society.* 28 (3), pp. 242–256.

Cottee, S. (2011) Jihadism as a subcultural response to social strain: Extending Marc Sageman's "bunch of guys" thesis. *Terrorism and Political Violence*. 23 (6), pp. 730–751.

Gartenstein-Ross, D. and Grossman, L. (2009) *Homegrown Terrorists in the U.S. and U.K.: An Empirical Examination of the Radicalization Process*. Washington DC: FDD Press.

Greene, W. (2010) Econometric models when there are rare events. Presentation for the 2010 Medici Summer School in Management Studies, New York University. Available at: http://pages.stern.nyu.edu/~wgreene/Econometrics-and-Rare-Events-Florence-2010-part-1.pdf. Accessed 9 September 2013.

Hacking, I. (1990) *The Taming of Chance*. New York: Cambridge University Press.

House of Commons (2006) *House of Commons Report of the Official Account of the Bombings in London on 7th July 2005.* London: HMSO.

Huey, L. (2011) Anti-surveillance activists v. the dancing heads of terrorism: The role of signal crimes, symbolic politics and sound bites in camera promotion. In Doyle, A., Lippert, R. and Lyon, D. (eds) *Eyes Everywhere: The Global Growth of Camera Surveillance*. London: Routledge, pp. 237–248.

Humphreys, A., Bell, S., Keidan, M. and Blackwell, T. (2013) How three Canadians graduated from a rebellious high-school friendship to the world of Islamist terrorism. *National Post*. Available at: http://news.nationalpost.com/2013/04/06/how-three-ontario-school-friends-grew-up-to-become-islamist-terrorists-in-north-africa/. Accessed 25 June 2013.

Horgan, J. (2005) *The Psychology of Terrorism.* London: Routledge.

Horgan, J. (2008) From profiles to pathways and roots to routes: Perspectives from psychology on radicalization into terrorism. *Annals of the American Academy of Political and Social Science.* 618 (1), pp. 80–94.

Innes, M., Abbott, L., Lowe, T. and Roberts, C. (2007) *Hearts and Minds and Eyes and Ears: Reducing Radicalization Risks through Reassurance-Oriented Policing.* Cardiff: Universities Police Science Institute.

Jackson, R. (2009) The study of terrorism after 11 September 2001: Problems, challenges, and future developments. *Political Studies Review.* 7 (2), pp. 171–184.

Jenkins, B. (2011) *Stray Dogs and Virtual Armies: Radicalization and Recruitment to Jihadist Terrorism in the United States since 9/11*. Santa Monica CA: Rand.

Kleinmann, S. (2012) Radicalization of homegrown Sunni militants the United States: Comparing converts and non-converts. *Studies in Conflict and Terrorism.* 35 (4), pp. 278–297.

Krueger, A. B. (2008) What makes a home-grown terrorist? Human capital and participation in domestic Islamic terrorist groups in the U.S.A. *Economic Letters.* 101 (3), pp. 293–296.

Kundnani, A. (2012) *Spooked! How Not to Prevent Violent Extremism.* London: Institute of Race Relations.

Lerner, R. M. (1987) A life-span perspective for early adolescence. In Lerner, R. M. and Foch, T. T. (eds) *Biological-Psychological Interactions in Early Adolescence.* Hillsdale NJ: Lawrence Erlbaum Associates.

Lichbach, M. I. (1998) Contending theories of contentious politics and the structure action problem of social order. *Annual Review of Political Science.* 1, pp. 401–424.

Lynch, O. (2013) British Muslim youth: Radicalization, terrorism, and the construction of the "other." *Critical Studies on Terrorism.* 6 (2), pp. 241–261.

MacCharles, T. (2013) Mauritania jailed Canadian Aaron Yoon for Al Qaeda ties, says Amnesty. *The Toronto Star*. Available at: www.thestar.com/news/canada/2013/04/05/aaron_yoon_serving_twoyear_sentence_in_mauritania_for_al_qaeda_ties_amnesty_international.html. Accessed 25 June 2013.

McCauley, C. (2012) Testing theories of radicalization in polls of U.S. Muslims. *Analyses of Social Issues and Public Policy.* 12 (1), pp. 296–311.

McCulloch, J. and Pickering, S. (2009) Pre-crime and counter-terrorism: Imagining future crime in the "War on Terror." *British Journal of Criminology.* 49 (5), pp. 628–645.

Porter, L. E. and Kebbell, M. R. (2011) Radicalization in Australia: Examining Australia's convicted terrorists. *Psychiatry, Psychology and Law.* 18 (2), pp. 212–231.

Post, J. M., Sprinzak, E. and Denny, L. M. (2003) The terrorists in their own words: Interviews with thirty-five incarcerated Middle Eastern terrorists. *Terrorism and Political Violence.* 15 (1), pp. 171–184.

Richards, A. (2011) The problem with "radicalization": The remit of "prevent" and the need to refocus on terrorism in the UK. *International Affairs.* 87 (1), pp. 143–152.

Rissland, E. L. and Xu, X. (2011) Using case-based tests to detect gray cygnets. *Case-Based Reasoning Research and Development.* 6880, pp. 258–273.

Sageman, M. (2004) *Understanding Terror Networks.* Philadelphia: University of Pennsylvania Press.

Sageman, M. (2008) *Leaderless Jihad: Terror Networks in the 21st Century*. Philadelphia: University of Pennsylvania Press.

Silber, M. (2011) *The Al Qaeda Factor: Plots against the West*. Philadelphia: University of Pennsylvania Press.

Silber, M. D. and Bhatt, A. (2007) *Radicalization in the West: The Home Grown Threat.* New York: New York Police Department.

Stroink, M. L. (2007) Processes and preconditions underlying terrorism in second-generation immigrants. *Peace and Conflict: Journal of Peace Psychology.* 13 (3), pp. 293–312.

Taleb, N. N. (2007) *The Black Swan: The Impact of the Highly Improbable.* New York: Random House.

Taylor, M. (2010) Is terrorism a group phenomenon? *Aggression and Violent Behavior.* 15 (2), pp. 121–129.

Tessler, M. and Robbins, M. D. H. (2007) What leads some ordinary Arab men and women to approve of terrorist acts against the United States? *Journal of Conflict Resolution.* 51 (2), pp. 305–328.

Wainer, H. (1976) Robust statistics: A survey and some prescriptions. *Journal of Educational Statistics.* 1 (4), pp. 285–312.

Williams, P. L. (2007) *The day of Islam: The Annihilation of America and the Western World*. Amherst, NY: Prometheus Books.

Wilner, A. and Dubouloz, C. (2010) Homegrown terrorism and transformative learning: An interdisciplinary approach to understanding radicalization. *Global Change, Peace and Security.* 22 (1), pp. 33–51.

Wilner, A. S. and Dubouloz, C. (2011) Transformative radicalization: Applying learning theory to Islamist radicalization. *Studies in Conflict and Terrorism.* 34 (5), pp. 418–438.

Volkan, V. D. and Harris, M. (1995) The psychodynamics of ethnic terrorism. *International Journal on Group Rights.* 3, pp. 145–159.

Zellner, A. (2007) Philosophy and objectives of econometrics. *Journal of Econometrics.* 136 (2), pp. 331–339.

4 Researching terrorism and counter-terrorism through a network lens

Martin Bouchard and Rebecca Nash[1]

Introduction

One of the most fundamental findings of terrorism research is that terrorists are, as far we can tell, normal people. Serious analysis of their background shows they are neither poor nor rich, and most are not particularly religious except for an escalation phase in the strength of their beliefs that seems to be happening in the period leading to an event (Bakker, 2006; Sageman, 2004). There is no clearly defined terrorist personality (Horgan, 2003), no simple profile to make individual-based predictions, and very little information available to distinguish the potential terrorist from the (relatively) non-violent supporter of a cause prior to a terrorist event.

These conclusions would not come as a surprise to criminologists who have found the same for criminals more generally. There are a host of risk factors predicting crime involvement, especially in adolescence, where criminal offending is relatively common (e.g., for reviews, see Farrington, 1998; Loeber and Hay, 1997). But the gap between possessing any risk factor and actually becoming a criminal is wide enough to prevent empirical tests from achieving anything resembling accurate predictions (Weisburd and Piquero, 2008). There is no crime "gene," both lower and upper social classes commit crime (although the poor are often over-represented in the criminal justice system), and although self-control may be lower for offending populations, it is not so much so that this characteristic is automatically associated with crime. In addition, many of the established sociological theories of criminal behavior start from the premise that there is little to distinguish criminals from non-criminals on fundamentals. Anomie theory, for example, establishes that a majority of individuals share similar values related to success, but that some (criminals) simply take illegal means (i.e., the means available to them) in order to reach that goal (Merton, 1938). Differential association theory focuses on behavior as opposed to individuals and posits that criminal behavior is learned the same way that most conventional behaviors are: that is, in the company of others (Sutherland, 1947). If the frequency, duration, priority and intensity of an individual's social interactions fall in favor of behavior on the illegal end of the spectrum, then that individual is more likely to adopt such behavior. The process is gradual, not

necessarily linear, and is a function of several interactions between social, psychological and contextual factors.

A similarly complex set of social, political, structural and opportunistic factors play a role in the trajectories of terrorists. To be sure, enough is known about terrorism and violent radicalization to imagine a point where it would be possible to make distinctions between terrorists and a relevant control group. Yet the kind of fine-grained, multi-level data and longitudinal research designs necessary to achieve this have yet to emerge. Among the slow discoveries of what makes a potential terrorist actualize his or her potential, scholars have increasingly found it hard to ignore the role of group processes and socialization in the etiology of terrorism. The social networks of friendships in which individuals are embedded, and how they identify with these social networks, have shown to be lines of research most worthy of attention in understanding pathways to terrorism (Sageman, 2004, 2008). If this assertion is valid, then detailed research into the nature and dynamics of the social networks of potential terrorists should be a top priority among terrorism scholars. This research would examine the social networks involved in preparing specific terrorist events (e.g., Everton, 2012; Koschade, 2006; Krebs, 2002; Magouirk *et al*., 2008; Rodriguez, 2005), but also those developed over the entire lifetime of terrorists—including those who share similar backgrounds but never get involved in violent actions. It would also look into the social interactions that happen offline and those occurring online, including the overlap between the two and careful examinations of the significance (or lack thereof) of online behavior on radicalization processes (Ducol, 2012). Ultimately, the field would also analyze continuity and change in the social networks of terrorists long after the initial events for which they became known, including in the time period following incarceration, as the convicted terrorists return to the community.

A concern for social interactions does not stop, however, at the terrorist and the networks in which he or she is embedded. The various law enforcement agencies involved in fighting terrorism are also interacting and cooperating together in investigations, and the nature of these social interactions is likely to have an impact on effectiveness in the field. The nature of group processes involved in teams of any kind have an impact on performance, and there is no reason to believe things are different for agencies involved in fighting terrorism.

In this chapter, we argue that integrating network concepts and network methods to the study of terrorism and counter-terrorism is of central importance in bringing the field forward from theoretical, empirical and policy perspectives. This is not exactly a new idea, although the move to study terrorist networks did not really take off until the events of 9/11 (Krebs, 2002). Such scholars as Marc Sageman were among the first to present a compelling argument for the use of network methods in the field of terrorism (Sageman, 2004, 2008). Pedahzur and Perliger (2011), Carley *et al.* (2003), Asal and Rethemeyer (2006), and Everton (2012) argued for a similar focus on the empirical study of terrorist networks, each emphasizing different aspects of the strengths of a network approach but also its limitations.

Notwithstanding these calls for the use of network methods in terrorism studies, a network approach to terrorism research is still not ubiquitous in the field, and many terrorism scholars do not come from fields with established training in social network methods (Pedahzur and Perliger, 2011). Valid network data is typically more difficult to access from open sources, making developments slower than desirable. The idea that networks can also be analyzed on the other side of the spectrum, within the agencies tasked with responding to terrorism, is also rarely discussed in terrorism studies. This chapter aims to contribute towards establishing network concepts and methods as critical to the development of the field.

Why study terrorism through a network lens?

Much like some of our predecessors (e.g., Perliger and Pedazhur, 2011), we believe that a network approach to the study of terrorism is one of the most productive ways forward for the field. There are at least three reasons why we think that this is the case. First, social ties and social influence have been argued to be central in the radicalization of individuals (Bakker, 2006; Hegghammer, 2006; Sageman, 2004, 2008). A compelling argument for this is the evidence that many friendship groups and social ties existed prior to devotion to a cause. Sageman (2008) describes two pathways to friendship and terrorism, incorporating data on the trajectories of two-thirds of his sample of 500 or so terrorists (pp. 66–67). The first pathway can be described as the collective decision of an existing friendship group to join the social movement and do something concrete for the cause. The second is the case of the immigrant joining old childhood friends in the host country. Although the initial goal of the interaction may have been companionship, the new member may be invited to participate in terrorist activities if such activities are part of what the old friends do.

Understanding the dynamics of group formation and social influence is the crux of social network analysis. The central assumption of social network analysis is that a detailed knowledge of the social structure in which individuals are embedded may be more informative in understanding behavior than common sets of attributes used to create profiles of individuals, such as age, gender, education or socio-economic status (Knoke and Yang, 2008). While research on group processes and small groups is informative in understanding identification, commitment and behaviors associated with group membership, the use of network methods to map and analyze the networks as they unfold provides an additional layer of precision in connecting social ties and their influence on behavior (or lack thereof).

Second, network methods allow for an accurate depiction of the internal organization of terrorist groups without potentially false assumptions about the ways these groups should function. A network approach does not impose a particular organizational structure or make assumptions about the division of labor within an organization. It lets the patterns emerge from the data, which opens up the possibility for unexpected findings, such as the discovery of information

brokers among the lower levels of an organization, or the realization that the channels of communication in hierarchical organizations do not always behave in the ways expected by theory (Morselli, 2009). In his initial analysis of 172 cases associated with Al-Qaeda and the Global Salafi Jihad, Sageman (2004) was shocked not to find evidence of top-down recruitment in the movement. As independent cases of homegrown terrorism became increasingly prominent in the years following 9/11, few people now expect to observe the type of recruitment expected of hierarchical organizations. The need to adopt methods that are amenable to tracking how individuals become embedded in these networks in the first place is even more salient than it was a decade ago.

Third, mapping terrorist networks can potentially improve the effectiveness of counter-terrorist measures. In fact, it is often the practical implications of adopting a network approach that motivates scholars to adopt network methods and that motivates law enforcement agencies to share data with these scholars. The idea is attractive because, in theory, network methods can precisely identify which actors should be removed in order to achieve maximum disruption (Borgatti, 2003; Everton, 2012; Joffres *et al*., 2011). In practice, the capacity of law enforcement agencies to accurately map a network as it exists prior to an intervention, and to base its target selection on it, is rarely reported in the literature. Most disruption network studies are simulations of different possible strategies to disrupt the network (Carley *et al*., 2003; Chen, 2012; Joffres *et al*., 2011; Roberts and Everton, 2011), or retrospective studies of what could have been done had network data been available prior to an intervention (Everton, 2012; Malm and Bichler, 2011). We come back to this literature in more detail below.

Conceptual clarification

The term "network" is used in different contexts to mean different things in terrorism literature, potentially creating confusion. The term "network" is used in at least two ways that may seem incompatible but in reality are not. First, the term is used to describe a mode of organization based on loosely structured affiliations, to be contrasted with formal hierarchies. Organizing as a "network" means that power and decision-making is not centralized to a single cluster of individuals in the organization, but rather spread horizontally over multiple clusters of actors who have reciprocal lines of communication (Powell, 1990). Network forms of organization are often seen as an adaptive response to environments where flexibility and efficiency are paramount, such as criminal and terrorist organizations (Morselli *et al*., 2007).

The term "network" is also used in a broader sense to refer to the study of any kind of social structure using network methods. When used in that context, hierarchies and informal groups alike can be analyzed as "networks"—the only criterion is for entities to connect in some form and in ways that are not entirely monotonic. Social network analysis is a set of methods for the study of relations among actors (Knoke and Yang, 2008), and such methods are thus suitable for almost any social context. And although the form and content of social

networks may be amenable to more surprises when studying informal organizations than hierarchical ones, prior studies have shown that a systematic mapping of social relations, even in hierarchies, almost always leads to some unexpected patterns of importance. Magouirk *et al*.'s (2008) analysis of the evolution of the network of Jemaah Islamiyah from its formation in the 1990s through the multiple attacks of the early 2000s showed how what was perceived as a relatively hierarchical organization controlled by one or two leaders became an increasingly decentralized group with multiple centers of gravity. The perception of Jemaah Islamiyah as "led" by a single person, however, remained alive for a long time (Magouirk *et al*., 2008). In their analysis of Palestinian suicide bomber networks, Pedazhur and Perliger (2006) also showed how following the leaders of these groups was unlikely to be a productive route of intervention. Instead, it is the brokers uncovered in the network who were most important in preparing successful attacks.

These two uses of the term are not incompatible, as "networks" may simultaneously describe a form of governance and a set of methods to describe the structure of social relations of any kind. Therefore, the qualifier used with the term is important (network organization vs. network methods). If the term is used on its own, however, the reader should have its broader meaning in mind. Unless otherwise specified, our use of the term refers to "network" in the broadest sense possible, to refer to a group of interconnected social entities of any shape or kind.

On the network implications of the leaderless jihad

Writing on the heels of the events of 9/11, Rothenberg (2002) made a series of assumptions about terrorist networks that served as a basis for subsequent publications by others (e.g., Tsvetovat and Carley, 2007). While he hardly had any strong data to back his assumptions, some later passed the test using empirical data many years after formulation. When he wrote his piece, Rothenberg had in mind the Global Salafi Jihad, in which a command component and a multiplicity of loosely connected cells, mostly independent, form the bulk of the network. The author formulated assumptions about terrorist networks based on the little knowledge available at the time. The first assumption, that *the entire global network is a connected component*, is of particular importance in light of the "old" and "new" findings on terrorist networks.

When he made this assumption, Rothenberg (2002) was not assuming that most individuals taking part in the network are actually connected to a majority of others around the world. He was merely stating that there is at least an indirect path from most individuals to a far-away, similarly minded cell. A good depiction of that idea was published two years later in Sageman's (2004) *Understanding Terror Networks*. The core of the network was the central staff formed around Bin Laden and his close allies. It was surrounded by three clusters loosely connected through the center: the Core Arabs, the Maghreb Arabs, and the Southeast Asian cluster.

Among the many assertions made about terrorist networks after 9/11, the global network assumption is perhaps the only one that failed to survive the test of time. This is not because Rothenberg (2002) was wrong at the time he wrote but because things changed fast after the events of 9/11. In fact, the Global Salafi Network presented by Sageman (2004) was argued in his subsequent book, *Leaderless Jihad* (Sageman, 2008), to have virtually disappeared. The Al-Qaeda (AQ) command center had been too risky to maintain, but more importantly, it was not necessary to have it. Instead, a transformation could be observed where "a multitude of local groups tried to emulate their predecessors by conceiving and executing operations from the bottom up" (Sageman, 2008, p. vii). This offered the idea of a leaderless jihad where local, homegrown terrorist groups form and plan attacks often without any direct connections or support from any command center, AQ or otherwise. This assertion does not deny that AQ leadership, in some form, may still exist. It simply argues that it does not have the same central brokering function it once had to facilitate terrorist attacks. From a practical standpoint, the more decentralized and diffuse the threat, the harder it is to prevent and detect. At the same time, homegrown terrorist groups tend to plan smaller, less lethal attacks than the AQ core groups (Helfstein and Wright, 2011; Sageman, 2008), which can be conceived as a sign of organizational failure (McAllister, 2004).

The truth is, the kinds of data required to test some of these assumptions have yet to surface. A proper test would map not only the social networks immediately involved in a particular attack but also the larger social circle of influence around each of the participants in the attack (ideally over a relatively long period of time). One of the criticisms of social network research is that it is sometimes difficult to determine the boundaries of the network (Morselli, 2009). Those chosen by the researcher appear to be artificially created, one way (e.g., arbitrary decisions by the researcher) or another (e.g., limits of the data). If the definition of social-tie inclusions is broad enough, the network to be constructed around actors of interest may indeed be extremely large—large enough to stop being meaningful, at least for immediate practical purposes. Yet mapping the larger social structure in which terrorists are embedded may be the only way to understand how they became considered as terrorists in the first place. It is also one of the most reliable ways of understanding the relative level of connections (or lack thereof) among those individuals self-identifying to the global social movement. Complicating matters even more, the social networks in which individuals are embedded also include contacts made online, especially those contacts deemed to be influential in their process of radicalization. While the role of the Internet should not be over-played as a *cause* of terrorism, its role as *facilitator* at key points in the trajectories of terrorists cannot be denied either.

Networks on the Internet

Terrorists are increasingly using the Internet to advance their goals and purposes (Coll and Glassner, 2005; Conway, 2002). The Internet allows terrorist groups to

form global networks of followers much beyond what their capabilities had been before the early 1990s (Lewis, 2005). The Internet offers: (1) easy access; (2) little or no regulation, censorship, or other forms of government control; (3) potentially huge audiences spread throughout the world; (4) anonymity of communication; (5) fast flow of information; (6) interactivity; (7) inexpensive development and maintenance of a web presence; (8) a multimedia environment; and (9) the ability to shape coverage in the traditional mass media (Weimann, 2006, p. 30). These characteristics of the Internet have allowed modern terrorist groups to connect, communicate, plan, target and command terrorist activities in a loosely connected, flexible and decentralized network structure. These types of networks are extremely hard to identify and infiltrate, making it difficult to implement appropriate measures for identification and interdiction purposes (Conway, 2006; Lewis, 2005; Weimann, 2006).

Advances in information technology are central in the creation of networks, including the new, decentralized terrorist networks emerging through their use of the Internet. By reducing the transmission time and cost of information shared over the Internet and by increasing the amount and complexity of the information stored and shared, these advances have allowed for dispersed terrorists to communicate and coordinate their activities through online chat rooms, computer conferencing, forums, blogs and personal websites (Zanini and Edwards, 2001). Coinciding with this view, Conway (2006) suggests that the Internet enhances terrorists' capabilities to transform their group structures and generate new links. Because of the alternative space the Internet provides for communication and discussion and because of the hypertext nature of the web, groups can link to their internal subgroups and external organizations around the globe from their central website in seconds.

There is little empirical research into the actual networks of terrorist offenders as they occur online. There are two lines of research in this area; one, seriously under-developed, focuses on individuals as they connect to others via online discussion forums or other social media (Ducol, 2012; Fu *et al*., 2010), and the other focuses on extremist groups' websites and their surrounding networks, usually extracted via the hyperlinks present on a website (Bouchard *et al*., 2014; Burris *et al*., 2000; Chen, 2012) but also via subscription to YouTube channels (Klausen *et al*., 2012). The research on online terrorist networks is best represented by the Dark Web project led by Hsinchun Chen (2012). In 2005, Zhou, Qin, Lai, Reid and Chen proposed a semi-automated methodology that combines the efficiency of automatic data collection and the accuracy of manual collection for identifying, classifying and organizing extremist website data. Starting from a seed website, the web crawler finds the hyperlinks found in the HTML of a web domain and follows them through in order to create the network. The end result is a network of web-servers, the webpages contained within them, and the links between these webpages such that the data retrieved on the Internet by the web crawler can be used to map and analyze terrorist and extremist networks (Bouchard *et al*., 2014). Important to note here is that the entire process described in the research by Chen and colleagues (2012) is

automatic, with little input from the user. The Dark Web project incorporates multilingual data-mining, text-mining and web-mining techniques to collect the most comprehensive collection of data generated by terrorist groups across the globe, including web sites, videos, forums, chat rooms, blogs and social networking sites (Chen, 2012). The Dark Web project has spawned several research studies on the nature of terrorists' use of the Internet and their online networks (e.g., Xu and Chen, 2008; Qin *et al*., 2006; Zhou *et al*., 2005, 2007). For example, Zhou, Qin, Lai and Chen (2007) developed a web-mining method for online extremist forums, while Xu and Chen (2008) applied network topological analysis methods to study the design of online terrorist networks. The merge of content and network analysis in researching these websites and forums has yet to be fully developed.

Terrorist network disruption: issues and prospects for counter-terrorism

One of the benefits of a network approach to terrorism is the opportunity to link it to intervention efforts, which we label here as network disruption studies. The starting point of disruption studies is to consider the removal of key nodes (or key links between actors, or clusters of actors) in the network in order to decrease the network's efficiency and, if possible, make the network dysfunctional. One issue with many disruption studies is the lack of theoretical guidance orienting the target selection process. Actors may be valuable to a network for a variety of reasons, and what distinguishes "key players" from actors that can more safely be ignored may depend on (1) the goals and priorities of law enforcement and (2) the capacity of the network to recover (i.e., network resilience). Actors can be valuable because they have many connections in the network (hubs), or because they connect otherwise unconnected parts or members of the networks (brokers), or because they bring unique resources to the network, whether these resources represent social, human or financial capital.

The majority of disruption studies include centrality measures but fail to consider in their assessment the resources or "value" that individuals bring to the network (Carley *et al*., 2003). Schwartz and Rouselle (2009) addressed this issue by designing a measure that notes both the structural location of an actor in the network and his or her "value" based on criteria relevant to the goals of the agencies planning the intervention. Labeled as "network capital," this measure takes into account both the structural location of actors and the resources they bring to the network based on parameters to be determined by the analysts. For online child pornography networks, for example, network capital includes the popularity of a website in numbers of other websites hyperlinking to it but also the severity of the content displayed on it (Westlake *et al*., 2011). For terrorist networks, it is easy to imagine a composite measure of network capital that includes both network importance and the quality or scarcity of the resources brought by an actor, including funds, a particular skillset such as bomb-making, or a unique

contact with a corrupt official (see Carley *et al*., 2003). Magouirk *et al.* (2008) certainly had some of these considerations in mind when they chose to represent the importance of actors in the Jemaah Islamiyah networks based on their reputation as opposed to their network centrality. Similarly, Roberts and Everton's (2011) construction of Noordin Top's network is a fine example of network scholars purposefully designing network data collection and coding strategies to take into account the wide variety of terrorists' roles and affiliations, offering a rare amount of flexibility to researchers thinking about disruption issues from a variety of angles. And their efforts at classifying network-oriented counter-terrorism strategies represent one of the few contributions of network disruption studies at both conceptual and practical levels. Still, much more work needs to be done to validate some of the assumptions built into their classification model, most likely in the form of evaluation studies where changes in terrorist networks are followed before, during and after intervention (Carley *et al*., 2003; McCulloh and Carley, 2011; Everton and Cunningham, 2013).

As Roberts and Everton (2011) remind us, any intervention against terrorist groups carries its fair share of risks and potential perverse effects. A purely data-oriented approach to network disruption may not capture the local sensibilities and other idiosyncrasies of a particular group and its situation and may thereby potentially exacerbate events. While a network approach is far from immune to errors and omissions, this approach also has the (rarely used) potential to examine and map what those unintended consequences may be well in advance of making an intervention. For example, it is possible to make a prediction on who is likely to replace a leader who has been killed or captured and how the network is likely to adapt post-intervention. Networks change over time (and some would say "all the time") for both endogenous and extragenous reasons, and the lessons emerging from full consideration of network dynamics on disruption have yet to permeate the field (for potential solutions, see Carley *et al*., 2003; Everton and Cunningham, 2013; Tsvetovat and Carley, 2005).

Conclusion

The deaths and destruction from the 9/11 terrorist attacks have left an indelible impression on the world. The events that unfolded on that day were the catalyst for the emergence of a "new" terrorism and the realization that current counter-terrorist measures are ill-equipped to combat this emergent terrorist threat. For instance, several researchers note that terrorist groups have shifted from rigid, hierarchical designs to more amorphous, horizontal, networked structures; in turn, this has impacted their operations, decision-making and targeting (Arquilla *et al*., 1999; Asal and Rethemeyer, 2006; Hoffman, 2002; Sageman, 2004; Zanini and Edwards, 2001). Before 9/11, Al-Qaeda was a centralized organization "with a clear, distinct center of gravity," with a very noticeable, outspoken core leadership (Sageman, 2004). However, after 9/11, and in response to traditional counter-terrorist measures today, terrorist groups such as Al-Qaeda have become decentralized, loosely connected networks. They appear resilient to traditional counter-terrorist measures

and have an increasing presence on the Internet (Conway, 2006; Denning, 2011; Lewis, 2005; Sageman, 2008). Counter-terrorism measures must adapt to the changing nature of the highly adaptive new terrorism, but only after it has gained a detailed understanding of the networks in which terrorists are embedded.

The importance of a network approach to the study of terrorism can be summarized in three points. First, networks are of great consequence in the whole life trajectory of terrorists—from the radicalization process to the planning and execution of terrorist events. Second, a network approach offers a more powerful framework to describe the variety of structures found in terrorist groups as they actually are. Third, approaching terrorist groups as networks allows researchers the opportunity to better measure concepts such as leadership and influence within the group, and allows for unexpected patterns in the sources of power within a group to emerge. Similarly, such an approach avoids making false assumptions about cohesion within the group (e.g., do all members know and interact with each other?) and the extent to which members of the group actually connect to a wider network of external influences (e.g., is Al-Qaeda Central indirectly involved in this attack?).

The improved understanding of terrorism via the network approach has important practical implications for counter-terrorism policies as well. For one thing, the effects of these interventions can be simulated and thus much better understood. And if the true sources of influence within terrorist networks are not solely the one derived from the leaders in name, then interventions targeting specific individuals stand to gain both in relevance and in potential effectiveness.

Note

1 The Canadian Network for Research on Terrorism, Security and Society (TSAS) provided partial funding to support the preparation of this chapter.

References

Arquilla, J., Ronfeldt, D. and Zanini, M. (1999) Networks, netwar and information-age terrorism. In Lesser, I., Hoffman, B., Arquilla, J., Ronfeldt, D., Zanini, M. and Jenkins, B. (eds) *Countering the New Terrorism*. Santa Monica CA: Rand, pp. 39–84.

Asal, V. and Rethemeyer, R. K. (2006) Researching terrorist networks. *Journal of Security Education.* 1 (4), pp. 65–74.

Bakker, E. (2006) *Jihadi Terrorists in Europe, their Characteristics and the Circumstances in which they Joined the Jihad: An Exploratory Study*. The Hague: Netherland Institute of International Relations/Clingendael.

Borgatti, S. P. (2003) The key player problem. In Breiger, R., Carley, K. and Pattison, P. (eds) *Dynamic Social Network Modeling and Analysis: Workshop Summary and Papers.* Washington DC: National Academy of Sciences Press, pp. 241–252.

Bouchard, M., Joffres, K. and Frank, R. (2014) Preliminary analytical considerations in designing a terrorism and extremism online network extractor. In Mago, V. and Dabbaghian, V. (eds) *Computational Models of Complex Systems*. New York: Springer, pp. 171–184.

Burris, V., Smith, E. and Strahm, A. (2000). White supremacist networks on the Internet. *Sociological Focus*. 33, pp. 215–235.

Carley, K., Dombroski, M., Tsvetovat, M., Reminga, J. and Kamneva, N. (2003) Destabilizing dynamic covert networks. In *Proceedings of the 8th International Command and Control Research and Technology Symposium, 2003.* Washington DC: National Defence University.

Chen, W. (2012) *Dark Web: Exploring and Data Mining the Dark Side of the Web*. New York: Springer.

Coll, S. and Glassner, S. B. (2005) Terrorists turn to the web as base of operations. *Washington Post.* 7 August. Available at: www.washingtonpost.com/wp-dyn/content/article/2005/08/05/AR2005080501138.html. Accessed 24 July 2012.

Conway, M. (2002) Reality bites: Cyberterrorism and terrorist "use" of the internet. Available at: www.firstmonday.org/Issues/issue7_11/conway/index.html. Accessed 22 August 2012.

Conway, M. (2006) Terrorist "use" of the Internet and fighting back. *Information and Security: An International Journal.* 19, pp. 9–30.

Denning, D. E. (2011) Terror's web: How the Internet is transforming terrorism. In Jewkes, Y. and Yar, M. (eds) *Handbook on Internet Crime*, pp. 194–213. Portland OR: Willan Publishing.

Ducol, B. (2012) Uncovering the French-speaking jihadisphere: An exploratory analysis. *Media, War and Conflict.* 5 (1), pp. 51–70.

Everton, S. F. (2012) *Disrupting Dark Networks.* Cambridge: Cambridge University Press.

Everton, S. F. and Cunningham, D. (2013) Detecting significant changes in dark networks. *Behavioral Sciences of Terrorism and Political Aggression.* 5 (2), pp. 94–114.

Farrington, D. (1998) Predictors, causes, and correlates of male youth violence. *Crime and Justice: An Annual Review of Research.* 24, pp. 421–475.

Fu, T., Abbasi, A. and Chen, H. (2010) A focused crawler for Dark Web forums. *Journal of the American Society for Information Science and Technology.* 61 (6), pp. 1213–1231.

Hegghammer, T. (2006) Terrorist recruitment and radicalization in Saudi Arabia. *Middle East Policy.* 13 (4), pp. 39–60.

Helfstein, S. and Wright, D. (2011) Covert or convenient? Evolution of terror attack networks. *Journal of Conflict Resolution.* 55 (5), pp. 785–813.

Hoffman, B. (2002) Rethinking terrorism and counterterrorism since 9/11. *Studies in Conflict and Terrorism.* 25 (5), pp. 303–316.

Horgan, J. (2003) The search for the terrorist personality. In Silke, A. (ed.) *Terrorists, Victims and Society: Psychological Perspectives on Terrorism and its Consequences*, pp. 3–28. Chichester: John Wiley and Sons Ltd.

Joffres, K., Bouchard, M., Frank, F. and Westlake, B. (2011) Strategies to disrupt online child exploitation networks. In *Proceedings of the EISIC—European Intelligence and Security Informatics*, pp. 163–170. Athens: Hellenic American University.

Klausen, J., Barbieri, E. T., Reichlin-Melnick, A. and Zelin, A. Y. (2012) The YouTube jihadists: A social network analysis of Al-Muhajiroun's propaganda campaign. *Perspectives on Terrorism*. 6 (1), pp. 36–53.

Knoke, D. and Yang, S. (2008) *Social Network Analysis.* 2nd edn. Los Angeles: Sage Publications.

Koschade, S. (2006) A social network analysis of Jemaah Islamiyah: The applications to counterterrorism and intelligence. *Studies in Conflict and Terrorism.* 29 (6), pp. 559–575.

Krebs, V. (2002) Uncloaking terrorist networks. *First Monday.* 7 (4).

Lewis, J. A. (2005) The Internet and terrorism. In *Proceedings of the Annual Meeting (American Society of International Law)*. 99, pp. 112–115. Washington DC: Lowes L'Enfant Plaza Hotel.

Loeber, R. and Hay, D. (1997) Key issues in the development of aggression and violence from childhood to early adulthood. *Annual Review of Psychology.* 48, pp. 371–410.

Magouirk, J., Atran, S. and Sageman, M. (2008) Connecting terrorist networks. *Studies in Conflict and Terrorism.* 31 (1), pp. 1–16.

Malm, A. and Bichler, G. (2011) Networks of collaborating criminals: Assessing the structural vulnerability of drug markets. *Journal of Research in Crime and Delinquency*. 48 (2), pp. 271–297.

McAllister, B. (2004) Al Qaeda and the innovative firm: Demythologizing the network. *Studies in Conflict and Terrorism.* 27, pp. 297–319.

McCulloh, I. and Carley, K. (2011) Detecting change in longitudinal networks. *Journal of Social Structure.* 12, pp. 1–37.

Merton, R. K. (1938) Social structure and anomie. *American Sociological Review.* 3 (5), pp. 672–682.

Morselli, C. (ed.) (2009) *Inside Criminal Networks*. New York: Springer.

Morselli, C., Giguere, C. and Petit, K. (2007) The efficiency/security trade-off in criminal networks. *Social Networks.* 29 (1), pp. 143–153.

Pedahzur, A. and Perliger, A. (2006) The changing nature of suicide attacks: A social network perspective. *Social Forces.* 84 (4), pp. 1987–2008.

Perliger, A. and Pedahzur, A. (2011) Social network analysis in the study of terrorism and political violence. *Political Science and Politics.* 44 (1), pp. 45–50.

Powell, W. W. (1990) Neither market nor hierarchy: Network forms of organization. In Handel, M. J. (ed.) *The Sociology of Organizations: Classic, Contemporary, and Critical Readings*, pp. 315–330. Thousand Oaks CA: Sage Publications.

Qin, J., Zhou, Y., Reid, E., Lai, G. and Chen, H. (2006) Analyzing terror campaigns on the internet: Technical sophistication, content richness, and web interactivity. *International Journal of Human-Computer Studies.* 65, pp. 71–84.

Roberts, N. and Everton, S. (2011) Strategies for combating dark networks. *Journal of Social Structure.* 12, pp. 1–32.

Rodriguez, J. A. (2005) The March 11th terrorist network: In its weakness lies its strength. Paper presented at the 8th Congreso Español de Sociología, Alicante.

Rothenberg, R. (2002) From whole cloth: Making up the terrorist network. *Connections.* 24, pp. 36–42.

Sageman, M. (ed.) (2004) *Understanding Terror Networks*. Philadelphia: University of Pennsylvania Press.

Sageman, M. (ed.) (2008) *Leaderless Jihad: Terror Networks in the Twenty-First Century.* Philadelphia: University of Pennsylvania Press.

Schwartz, D. M. and Rouselle, T. (2009) Using social network analysis to target criminal networks. *Trends in Organized Crime*. 12 (2), pp. 188–207.

Sutherland, E. H. (1947) *Principles of Criminology*. 4th edn. Chicago: Lippincott.

Tsvetovat, M. and Carley, K. (2005) Structural knowledge and success of anti-terrorist activity: The downside of structural equivalence. *Journal of Social Structure.* 6, pp. 1–38.

Tsvetovat, M. and Carley, K. (2007) On effectiveness of wiretap programs in mapping social networks. *Computational and Mathematical Organization Theory.* 13, pp. 63–87.

Weimann, G. (2006) *Terror on the Internet: The New Arena, The New Challenges.* Washington DC: United States Institute of Peace.

Weisburd, D. and Piquero, A. (2008) How well do criminologists explain crime? Statistical modeling in published studies. *Crime and Justice: An Annual Review of Research.* 37, pp. 453–502.

Westlake, B., Bouchard, M. and Frank, R. (2011) Finding the key players in online child exploitation networks. *Policy and Internet.* 3 (6), pp. 1–32.

Xu, J. and Chen, H. (2008) The topology of dark networks. *Communications of the ACM*. 51, pp. 58–65.

Zanini, M. and Edwards, J. A. (2001) The networking of terror in the information age. In Arquilla, J. and Ronfeldt, D. F. (eds) *Networks and Netwars: The Future of Terror, Crime and Militancy.* Santa Monica CA: RAND Corporation.

Zhou, Y., Qin, J., Lai, G. and Chen, H. (2007) Collection of U.S. extremist online forums: A web mining approach. In *Proceedings of the 40th Hawaii International Conference on System Sciences*, *Waikoloa, Hawaii, January 3–6, 2007*.

Zhou, Y., Qin, J., Lai, G., Reid, E. and Chen, H. (2005) Building knowledge management system for researching terrorist groups on the web. In *Proceedings of the Eleventh Americas Conference on Information Systems*, *Omaha, NE, August 11–15, 2005*. Red Hook NY: Curan Associates Inc., pp. 2524–2536.

5 Travel broadens the network

Turning points in the network trajectory of an American jihadi

Rebecca Nash and Martin Bouchard

Introduction

Omar Hammami (Abu Mansoor al-Amriki, or "the American") was a homegrown terrorist from the United States who, between the years of 2007 and 2013, fought a personal jihad against the country in which he was born (FBI, 2012). His gradually more radical views turned violent soon after he arrived in Somalia in 2006 and met up with several jihadi brothers who shared his socio-political ideologies and hunger for jihad against the West. Hammami rose in the ranks of Al-Shabaab, an international terrorist group based in Somalia with ties to Al-Qaeda and identified as a terrorist organization by the United States (BBC, 2013; Dagne, 2011). Due to his specialized computer knowledge, his understanding of the Internet as a recruiting tool, and his being an American-born English speaker, he become, according to his own report, a commander and head propagandist in Al-Shabaab (Hammami, 2012). According to a BBC news report, Hammami was murdered in September 2013 by members of Al-Shabaab, the organization he was supporting (BBC, 2013).

The present study maps the personal (ego) network of Hammami in order to follow his radicalization process and journey to terrorism. We aim to detect influential individuals as well as specific turning points that may be considered crucial to his radicalization process, both of which have been demonstrated as key to the radicalization processes of numerous homegrown terrorists (Bakker, 2006; Brooks, 2011; Jenkins, 2011; Sageman, 2008, 2004; Southers, 2013; Hegghammer, 2006). As far as the authors know, this is the first study to use social network analysis to map the network of a homegrown terrorist during his full radicalization trajectory.

Homegrown terrorism and the radicalization process

The number of homegrown violent extremists or homegrown terrorists from the West, including Australia, Canada, Europe and the United States, has been increasing since 2001 (Gartenstein-Ross and Grossman, 2009; Wilner and Dubouloz, 2010). Most definitions of what constitutes homegrown terrorism converge on the core concept of a terrorist offender attacking targets belonging

to his/her own country. In this chapter we adopt Wilner and Dubouloz' (2010) definition of homegrown terrorists as "perpetrators who are citizens or residents born, raised, and educated within the countries they attack" (p. 1), a definition which is consistent with, yet broader than, others (e.g., Beutel, 2007; Brooks, 2011; Krueger, 2008; Southers, 2013; Precht, 2007; Crone and Harrow, 2011).

The extant literature is not clear on whether specific factors can help differentiate homegrown terrorists from individuals who never resort to acts of violence. For example, much of the literature on homegrown terrorists suggests that they are male, Islamic and of lower socio-economic status, that they have a difficult time integrating into the larger community due to their religion, that they face discrimination and xenophobia, and that they have a sense of alienation due to their being caught between different cultures and a lack of belonging (Beutel, 2007; Wilner and Dubouloz, 2010). However, Sageman (2004) found in a sample of 172 homegrown terrorists that, on average, they come from middle-class homes, are educated and have caring families. There is, quite simply, no consistent terrorist profile (Horgan, 2003).

The differences in the literature shed light on our superficial understanding of what makes a person turn his/her socio-political and religious ideologies into violent acts of terrorism against civilians within their own countries of origin. Radicalization is the process of committing oneself to a particular belief system and to the imposition of that belief system on society with violent acts; it is, therefore, a precursor to terrorism (Jenkins, 2009; Gartenstein-Ross and Grossman, 2009; Powers, 2014; Southers, 2013). Very little may distinguish individuals who radicalize from those who do not, as suggested in Sageman's (2008) definition: radicalization is the "process of transforming individuals from rather unexceptional and ordinary beginnings into terrorists with the willingness to use violence for political ends" (p. vii). An event or experience in an individual's life begins with some injustice or tribulation which makes them susceptible to extremist ideologies (Southers, 2013). Southers (2013) explains that these feelings of injustice or tribulation may begin through several factors including conflicted identities, oppression and socioeconomic exclusion.

Many scholars have attempted to define the radicalization process as a series of steps that go from the broad to the specific. Not all of them emphasize the role social networks may play in this process, but many have integrated the possibility of mentors, religious authorities, and other influential social ties being key to the process. For example, Gartenstein-Ross and Grossman (2009) suggest that there are six indicators of the process from radicalization to violence: (1) adopting a legalistic interpretation of Islam; (2) trusting only select religious authorities; (3) perceiving a schism between Islam and the West; (4) low tolerance for perceived theological deviance; (5) attempting to impose religious beliefs on others; and (6) political radicalization. Gartenstein-Ross and Grossman (2009) found that 20 percent of their sample of homegrown terrorists had a spiritual mentor, while 25.6 percent had an influential individual in their lives who sanctioned violent activity through perceived religious authority (p. 14).

Wiktorowicz (2004) suggests a four-step process for the radicalization process of homegrown terrorists in which "socialization" with radicalized others is the last step. These steps are: (1) a cognitive opening, which consists of a lack of integration into society along with issues of self-identity leading to receptiveness to new ideologies; (2) religious seeking, stemming from a lack of religious knowledge, which helps individuals apply meaning to their newfound ideologies; (3) framing, in which the "radical" group's ideologies "make sense" to the individual and thus are accepted by the individual; and (4) socialization, where the individual engages in religious indoctrination (p. 1). Beutel (2007) suggested that Wiktorowicz's (2004) four-step process explains that radicalization is "internalized and reinforced by others who share the same views" but reproached Wiktorowicz for limiting the radicalization process to only face-to-face interaction without regard to the role of the Internet (p. 2).

Wilner and Dubouloz' (2010) three precursors to radicalization are interesting in that they suggest the gradual replacement of one social network (e.g., non-radicals or moderates) for another. The first precursor is socio-political alienation—the stage when individuals isolate themselves from the broader community and begin to identify with others who share the same ideologies. The authors write that they "seek other like-minded individuals to associate with [and] in so doing they construct a narrow social network … distinct from the broader societal one" (Wilner and Dubouloz, 2010, p. 38). The second precursor mentioned by the authors is religiosity and globalization; the third is reaction to foreign policy. All of these characterize Omar Hammami's trajectory one way or another.

Case study: Omar Hammami

Omar Shafik Hammami comes from a mixed religious and ethnic background. His mother is Caucasian and a practicing Christian from the southern United States, holding deeply religious ideologies. Her parents were also practicing Christians. Hammami's father is Syrian and comes from a family who followed the traditional Arab culture. Hammami's father, however, is not at all religious. Hammami's grandfather on his father's side was a businessman who was also not religious; Hammami believes this aspect of his family to be an important part of who he is now because he was not raised as a Muslim, but instead as a Christian. During his youth he attends a Christian church but withholds this from his father due to his father's non-religious status. It is not until Hammami visits his father's family in Syria when he is in eighth grade that he is introduced to Islam—his Syrian family teaches Hammami how to pray and to read from the Qur'an. Hammami's trip to Syria to meet his family is a significant turning point in his life; Hammami asserts that he felt very comfortable and spiritually close to his Muslim family and toward Islam at this point (Hammami, 2012).

Hammami's father eventually discovers that he is secretly attending a Christian church with his mother and, in frustration, introduces Hammami to a shaykh in Daphne, Alabama, where they are living, to learn about Islam instead. The

shaykh compels Hammami to change his dress habits, his prayer habits and his thoughts about the "global persecution of Muslims" (Hammami, 2012). It is at this time that Hammami starts a Muslim club in high school for fellow students to practice Islam, to pray, and to read and discuss the Qur'an with other like-minded individuals. It is also at these meetings that Hammami meets his best friend (later labeled as FJ1[1]), a fellow student with whom Hammami eventually converts to Islam. The forming of this friendship tie, which becomes a kinship tie (Hammami later marries FJ1's sister and has a daughter), is a turning point in Hammami's life, in his feelings toward Islam and in his progression from radicalization to violence. Hammami soon drops out of University and moves to Canada with FJ1; the two believe that in Canada they will gain a deeper understanding of Islam and jihad away from the overwhelming prejudice they have faced in the United States. Hammami marries his first wife in Toronto.

While in Canada, Hammami attains work through Somali ties and befriends an Egyptian citizen through whom he learns about the persecution of Muslims in Somalia by Christians (the West) and who eventually leads Hammami and FJ1 to Alexandria, Egypt. After a short time in Toronto, Hammami then moves to Alexandria with his wife, FJ1 and FJ1's family to be in "the land of the Muslims" where he can focus more deeply on jihad (Hammami, 2012). In Alexandria, Hammami establishes contact with a Salafi Qur'an teacher who guides Hammami on what it is to be a Salafi Muslim.[2] While in Egypt, Hammami also meets FJ2, who becomes a major influence in Hammami's life in taking the step from radicalization to violent acts of terrorism. FJ2 is also an American-born Muslim and homegrown terrorist who fought jihad in Somalia. In 2007, FJ2 was sentenced to 10 years in prison on charges of receiving military training from a known terrorist organization, Al-Shabaab (FBI, 2007). The two become best friends while in Egypt, and together they travel to Somalia in 2006 (FBI, 2007; Hammami, 2012) and join Al-Shabaab.

While serving as a commander, recruiter and propagandist within the ranks of Al-Shabaab, Hammami continues to make many influential contacts including close ties to Islamic fundamentalist leaders within Al-Shabaab, some with ties to Al-Qaeda (Dagne, 2011). During this time, however, in-fighting among the leaders of Al-Shabaab leads to a split in 2012 between the Asmara group (Hizbul Islam) and the Xarakah ash-shabaab al-Mujaahidiin faction (Dagne, 2011; Hammami, 2012; Mohamed, 2012). Hammami's Islamic extremist ideologies lead him to follow Xarakah ash-shabaab al-Mujaahidiin, further isolating himself among a smaller group of Islamic militant extremists consisting of jihadi leaders and guerilla fighters who are described as sharing similar radical ideologies to that of Al-Qaeda (Mohamed, 2012).

Current study

In *Leaderless Jihad*, Sageman (2008) argued that focusing on the dynamics of social networks and how networks influence individuals to become terrorists offers the best approach to understanding the phenomena of homegrown

terrorism and violent extremism. The chapter by Bouchard and Nash in this volume shows that there has been an increase in the use of social network theory and methods by law enforcement agencies world-wide in understanding terrorist networks and as an application for implementing counter-terrorist measures (Carley, 2007; Everton, 2012; Koschade, 2006; Krebs, 2002; Rodriguez, 2005; Sageman, 2004, 2008; Toth *et al*., 2013; Xu *et al*., 2009). Most of these contributions focus on a specific attack or organization. None, to our knowledge, applied network methods to study the full trajectories of violent radicalized individuals, as we propose here.

The analysis of personal (ego) networks can be used to uncover actors (or clusters of actors) who are highly central in the trajectory of an individual and who are thus important in changing that individual's behavior. Sageman (2004), who collected data on over 400 terrorists, found that the social structures of their networks were instrumental in recruiting young men to commit terrorist acts and played a pivotal role in their success as homegrown terrorists. In Omar Hammami's trajectory, we were able to uncover a variety of contacts who aided him first in gathering knowledge of Islam, who influenced him in adopting a violent narrative towards the West, and who helped him learn technical skills to make weapons, including individuals he interacted with in training camps and on the Internet to learn military and guerilla fighting skills. Network analysis gives researchers, law enforcement agents and policy-makers the ability to uncover complex patterns and relationships within an individual's or group's social network and to illustrate these networks in simple, visual representations in order to identify patterns of behavior and key individuals who may be influential in changing behavior.

This chapter applies social network analysis to map and create the ego network through time of Omar Hammami, a homegrown terrorist, utilizing data obtained from a self-published autobiography from the time period of Hammami's early childhood (approximately the late 1980s) to September 2012 (the date of publication of this autobiography). The aims are (1) to obtain visualizations of Hammami's main ego network and subsequent networks through time, and (2) to identify influential individuals and specific events which were crucial to Omar Hammami becoming a homegrown terrorist working in the ranks of Al-Shabaab. As stated by Morselli (2001), egocentric network data drawn from such sources provides a

> chronology of a participant's evolution from his initial entry into a given illegal activity, gradual rise and establishment of a reputation, and eventual fall … taking place via a contact to contact narrative pattern … the aim should be toward identifying various transitions, events, or outcomes.
>
> (Morselli, 2001, p. 210)

Social networks allow us to pinpoint key players and events which in turn provide information helpful in implementing counter-terrorist strategies in the reduction and prevention of the radicalization of homegrown terrorism (Sageman, 2008; Southers, 2013).

Data and methods

Constructing the network

The data and personal ego network for this study were first extracted from Omar Hammami's (2012) Internet-published autobiography: *The story of an American jihaadi: Part one.* Presented with the unique opportunity provided by the publication of this memoir from a homegrown terrorist from the United States, we follow Morselli's (2001, 2003) approach in applying network analysis to autobiographical data. Historical and/or archival data are beneficial to network studies because these types of sources are generally longitudinal in nature, telling a story from beginning to end (Borgatti *et al*., 2013). We trace social ties and events through time, ties influential in Hammami's acceptance and practice of Islam, his desire to become "a pure Muslim," and his journey to engage in jihad. Conversely, we excluded any contacts that were not mentioned as significant, including jihadi brothers who were not reported as more than passersby. The archival data used in this study allows us to follow the dynamic nature of Hammami's radicalization over time, providing insightful information on key individuals who introduced him to Islam during grade school and individuals who traveled with him to Canada, to Egypt, and finally to Somalia where he would join with many highly influential members of Al-Shabaab, many of whom are wanted for acts of terrorism by the United States and other Western nations. While no specific dates or time periods were mentioned within the autobiography, it is written following a linear perspective through time, and thus events could easily be extracted over time through significant places Hammami traveled to during his radicalization process.

Secondary sources were an integral part of the current study to identify specific dates in the timeline and triangulate the roles of individuals in Hammami's network. Secondary data sources include information obtained from the Federal Bureau of Investigation (FBI), as well as other US government documents, peer-reviewed journal articles, and news sources from around the world such as the *New York Times* and the BBC, many of which are cited directly throughout the chapter where relevant (BBC, 2009, 2013; Dagne, 2011; FBI, 2007, 2012; Mohamed, 2012; US Department of the Treasury, 2000). These sources allowed us to construct an approximate timeline of important events and to identify specific terrorist groups active during this time period. We also used data triangulation to identify the roles and importance of specific actors within these groups who influenced the trajectory of Hammami's radicalization and eventual progression to violent extremism. Secondary data sources provided information on Hammami himself, specific dates and names, and the roles of many of the influential people in Hammami's life which were not provided in the autobiography. Secondary sources also provided the ability to cross-check the authenticity of information about specific contacts and events in the different networks created from Hammami's autobiography. With the exception of unnamed individuals in the autobiography, information about family, friends, Al-Shabaab jihadists and

leaders of Al-Shabaab were confirmed through secondary sources. Hammami (2012) mentions the split between the two differing factions of Al-Shabaab in 2010 and that he was aware that some members of the Asmara group faction were unhappy with his "behavior." This information was also confirmed through secondary sources, leading us to be confident in the accuracy of information provided in Hammami's autobiography.

Timeline

The estimated time period for Hammami's working network begins in the late 1980s during his early childhood. Between 1997 and his high school graduation year in 2001, Hammami travels to Syria to visit his father's side of the family for the second time, openly practices Islam on campus and founds an Islamic study group for fellow students to learn the writings of Muhammad. In 2004, Hammami and his friend FJ1 move to Toronto, Canada. In approximately 2005, Hammami, FJ1 and their wives and children move to Alexandria, Egypt (this important event may have occurred in 2004 since the pair did not spend a full year in Toronto), where he meets his friend FJ2 who, in 2006, travels with Hammami to Somalia to cross the boundary and engage in violent acts of terrorism in the name of Islam. Two other important dates are 2007 and 2009 when Hammami is seen on television and in an online video discussing jihad, recruiting others to join the fight for jihad and engaging in fighting/training activities—these last two dates are the only proof after 2006 that his family knew that Hammami was still alive. According to the BBC (2013), several sources in Somalia provide information that Omar Shafik Hammami was killed by members of Al-Shabaab on 12 September 2013.

Locations

A node list including each contact influential to Hammami was created to map his overall network. The data were organized around the roles played by the individual in relation to Hammami and the location(s) where these ties were active in his network. We coded for six specific locations, which act as six consecutive time periods (and turning points) in Hammami's trajectory. The six locations are (1) Daphne, Alabama, which encompasses his family and school life; (2) Toronto, Canada, where he meets his first wife and develops important ties to the Somali–Canadian community; (3) Alexandria, Egypt, where he meets his best friend FJ2 (see below), who is his tie to Al-Shabaab in Somalia; (4) Mogadishu, Somalia, where he begins travelling with Al-Shabaab members and committing act of violence for the first time; (5) Chiamboni, Somalia where he receives advanced training to fight in jihad: and (6) Baraawe, Somalia, where he starts a new phase of his journey to jihad by joining the Islamist militant group Harakat ash-shabaab al-Mujahideen, created after a major split in factions occurred on the governance of Somalia and its people (Hammami, 2012; Mohamed, 2012).

Types of ties

Characteristics of ties were recorded by relationship to Hammami and include family (F), friends (FR), jihadi brothers (J), jihadi leaders (JL), and religious/teachers (M or S).[3] In addition to his family members, the 15 family ties in the network include Hammami's two wives and two children, and also their family members where relevant. Friends were coded as such if they were significant to Hammami's trajectory but the friendship developed prior to the start of his radicalization process. One (FJ1) of the 11 friends followed Hammami to Egypt and started his own radicalization process, but the others remained outside of this aspect of Hammami's life. Jihadi brothers ($n=25$) held no special status or rank within Al-Shabaab, while "leaders" ($n=15$) had decision-making power over individuals, whether operationally or ideologically. Finally, influential Muslim shaykhs were grouped with two high-school teachers (not necessarily religious) named by Hammami as highly significant in his motivation for life-long learning as a single category of six religious/teacher contacts.

Network measures

The network data was undirected, meaning that all ties were assumed to be reciprocal. The source material did not allow us to provide specific values to the ties in the network, but we could reliably code for presence or absence of a relationship. Two network measures were also utilized to describe Hammami's network over time in order to better understand his individual radicalization to recruitment into Al-Shabaab: (1) network density, and (2) betweenness centrality. Density is the number of ties present in a network, expressed as a proportion to the total number of ties possible. High density indicates a cohesive network where a majority of contacts know all others. Centrality can be thought of as the relative contribution an actor makes to the structure of the network, or his/her importance. This study focuses on the network measure of betweenness centrality to identify those individuals who were integral in introducing Hammami to other influential people and those individuals who were in a position to control information. Betweenness centrality is measured as the number of times an actor in a network lies on the geodesic (shortest path) between all other actors in the network (Freeman, 1979). Betweenness centrality identifies brokerage positions or actors who are connecting otherwise unconnected actors in a network. Their centrality score comes from their strategic position between other actors in the network, thus controlling the flow of information or influence within a network. The data were analyzed using UCINET 6.0 (Borgatti *et al*., 2002).

Results

Hammami's journey to jihad—the overall network

Figure 5.1 represents Hammami's overall ego network, encompassing 71 individual contacts who were influential throughout his journey to radicalization,

including his pre-jihad network of friends and family. Each actor in the network is designated by their relationship to Hammami. Family are represented by squares, friends by circles, jihadi brothers by up-triangles, jihadi leaders by down-triangles, and religious teachers represented by a diamond symbol. Family members make up 21.1 percent of the total network, friends represent 15.1 percent, jihadi brothers 33.8 percent, jihadi leaders 21.1 percent, and religious/teachers contacts make up 8.5 percent of his network. The density of the overall network is 0.1451; that is, 14.5 percent of all possible ties in Hammami's network are present. The density measure and Figure 5.1 suggest a loosely connected network with multiple clique-like structures of highly connected contacts who all know each other.

There are two other important observations to make from examining Hammami's full network in Figure 5.1. First, we can see a clear disconnect between Hammami's pre-jihad network and his Somalia networks, with three distinct subgroups capturing the majority of the contacts in his network. Hammami's pre-jihad network of family and friends, visible at the top of Figure 5.1, represents his pre-jihad days. This network includes his immediate family members but also his high school friend FJ1, with whom he starts his journey to jihad. All members of this sub-group were influential in bringing Hammami first to Canada

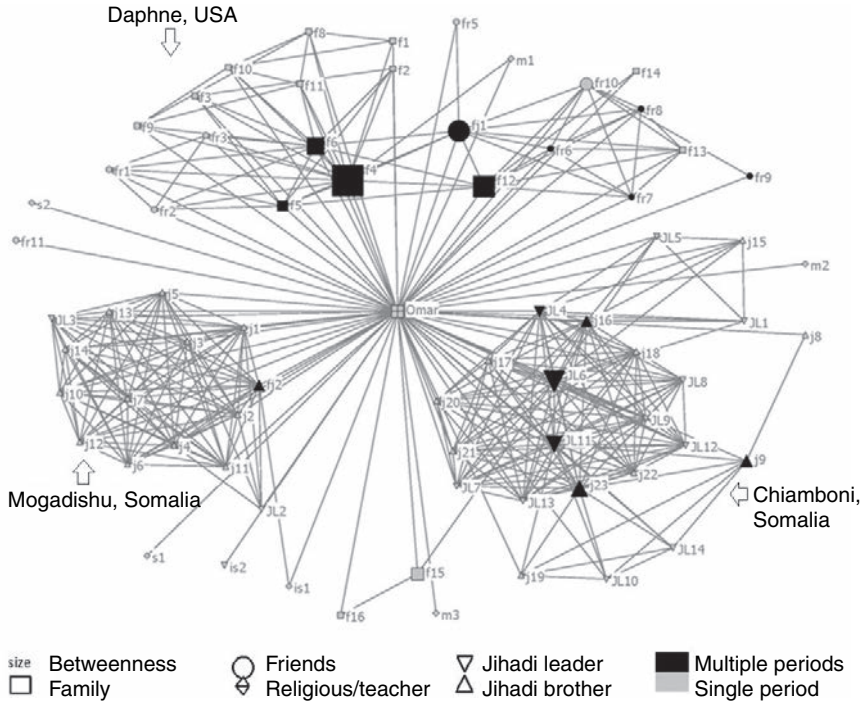


Figure 5.1 Full personal network of Hammami from his pre-jihad days to Al-Shabaab ($n = 72$).

and then to Egypt, where he would gain a deeper understanding of his Islamic ideologies as well as make contacts with ideologically like-minded individuals.

The second subgroup, found on the left of Figure 5.1, we have labeled as the Mogadishu network. This highly dense group was mostly formed in this Somalian city, the first visited by Hammami after he left Egypt. Among the 15 contacts in that subgroup we find 13 jihadi brothers, including Hammami's friend and fellow homegrown terrorist FJ2, whom he originally met in Egypt. The subgroup also includes two leaders, JL2 and JL3. Secondary sources reveal that JL3 was a moderate leader of the Islamic Courts Union (ICU) and was opposed to the militant ideologies of Al-Shabaab (BBC, 2009; Dagne, 2011). All of the individuals in the second subgroup were instrumental in Hammami's turn from radicalization to recruitment into Al-Shabaab. But it was with the third subgroup (labeled as the Chiamboni network), on the right side of Figure 5.1, that Hammami began his jihad and committed violent acts of extremism for the first time. This group involved a mix of jihadi brothers and leaders. It included JL6, leader of Al-Shabaab and the *mujahidin* movement, and J16, who owned the jihadi headquarters where recruited individuals went for training in guerilla fighting tactics. Hammami's ties to the individuals in this subgroup were instrumental in teaching him tactics for fighting more effectively, allowing him to move further up in the ranks of Al-Shabaab. Hammami became very close with JL6, who enabled him to become a commander in Al-Shabaab; he began to recruit and train others to commit acts of violence.

The second important observation from Figure 5.1 is that it allows us to identify and locate the individuals who facilitated Hammami's integration to new networks as he traveled from the USA to Somalia. We calculated the betweenness centrality scores of all contacts in the full network and used these scores to represent node size in the network. Outside of Hammami himself, 10 other actors stood out for having high betweenness centrality scores, suggesting a brokering or bridging role for them in Hammami's journey. Table 5.1 lists these 10 others, showing their relation to Hammami as well as the locations in which they were active members of his network.

These 10 actors are important given our focus on turning points and Hammami's multi-country journey to jihad. Some of the most important actors in terms of betweenness centrality (his father, sister and first wife) were not necessarily from his jihad days. For example, his father shared ties to Hammami's immediate family, his Syrian family and many of Hammami's friends in high school. The time period Hammami was in contact with his father (the late 1980s to approximately 2004 to 2005 when he moved to Alexandria, Egypt) was also the period of his radicalization process, during which he met many new contacts that were influential on his journey to jihad.

Another observation is that all of these brokers helped Hammami bridge time periods, with representatives from all five transitions:

1 from Daphne to Toronto (F4, F6, FJ1, F12);
2 from Toronto to Alexandria (FJ1, F12);

Table 5.1 Top 10 brokers in Hammami's full network[a]

ID	*Relation to Hammami*	*Locations where contact is active*	*Betweenness score*[b]
F4	Family (father)	Daphne and Toronto	1.13
JL6	Jihadi leader	Mogadishu and Chiamboni	0.70
JL11	Jihadi leader	Chiamboni and Baraawe	0.70
J23	Jihadi brother	Chiamboni and Baraawe	0.70
F6	Family (sister)	Daphne and Toronto	0.48
FJ1	Best friend 1	Daphne, Toronto and Alexandria	0.38
F12	Family (first wife)	Daphne, Toronto, Alexandria and Mogadishu	0.38
JL4	Jihadi leader	Mogadishu and Chiamboni	0.36
J16	Jihadi brother	Mogadishu and Chiamboni	0.36
FJ2	Best friend 2	Alexandria and Mogadishu	0.34

Notes
a Ranking excludes Hammami, who inevitably ranks first on that measure.
b Raw score.

3 from Alexandria to Mogadishu (F12, FJ2);
4 from Mogadishu to Chiamboni (JL6, JL4, J16);
5 from Chiamboni to Baraawe (JL11, J23).

The contacts bridging the last three transitions are especially important because many of those vouched for Hammami as he made his way to Al-Shabaab in Somalia.

One last observation from Figure 5.1 is necessary before moving to the next section of our analysis. Much work in social network analysis is focused on central actors, but in some cases the peripheral actors are just as important, if not more so, than certain central participants. In criminal networks, this occurs when the leaders take a peripheral role to avoid the increased risks of detection that come from being in the thick of things (Morselli, 2009). Many of the peripheral actors in Hammami's network were among the most influential in his journey: not necessarily in connecting him to new social networks, but in influencing his own views and resolve to participate in jihad. For example, five of the six religious/teacher contacts (M1, M2, M3, S1, S2) are isolated dyads in the network and do not occupy particularly strategic positions from that perspective. The exception is a key Internet source, IS1 (bottom center of the network in Figure 5.1), who was also connected to Hammami's friend FJ2 who traveled with him from Alexandria to Mogadishu. IS1 was an extremely influential Salafi scholar who had been reported to use his website for recruitment purposes (McCants *et al*., 2006). In his autobiography, Hammami states that he realized that jihad is an obligation and that he himself had become a jihadi after reading IS1's books on his website (Hammami, 2012, p. 34). Hammami's Salafi Qur'an teacher (M2) and the shaykh (M3), both of whom he met in Alexandria, were highly influential in cultivating his socio-political ideologies about Islam and what it meant to become a pure Muslim. Actors S1 and S2 were also influential to Hammami on

an intellectual level in that they taught him to be open-minded in accepting other religions, which was when he began to learn about Islam (as he had grown up a Southern Baptist). Referring to S1, Hammami states that "She gave me a passion for learning. Or at least she increased that passion. And she had us study other religions and ideologies as well" (Hammami, 2012, p. 11).

Turning points and evolution of the network over time

Examining the evolution of Hammami's network over time allows us to better appreciate the turning points that occurred in his strategy and their consequences for his radicalization process. First, we broke down the network based on the six time periods and locations and labelled consecutive time periods to illustrate the nature of the transitions that occurred in Hammami's personal network over time. Figure 5.2 presents his network in the first years of his life living in Daphne Alabama (t1) and then Toronto, Canada. Hammami's pre-jihad network resembles the network of any young man his age, except that it also illustrates the dual religious environment he grew up in, which may have played a role in his radicalization process. One of the most central actors was Hammami's father (F4), at the center left of the network. F4's strategic position in this network is not surprising as he introduced Hammami to both his Syrian family (actors F9, F10, and F11 at the lower left) and the local shaykh in Daphne (actor M1). These contacts proved to be extremely influential, with Hammami eventually giving up his Baptist upbringing, which had been guided by his mother, and embracing Islam. Hammami's cousins in Syria introduced him to the Qur'an and the writings of Muhammad. The local shaykh in Daphne (M1) taught him how to pray and study Islam during his high school years—this became a significant turning point in Hammami's life, as before this point he had fully considered himself a Baptist due to the influence of his mother's religious interests. Being caught between different cultures, religions or political organizations can give some individuals a sense of alienation and a lack of belonging which is associated, for a minority, with the beginning of the radicalization process.

Figure 5.2 also includes Hammami's Toronto network (right side of the diagram), including his high-school and college friend FJ1, who remained in his network up to and including the major turning point when Hammami's trajectory took him to Egypt. Another important actor in his pre-jihad network was FR5, whom Hammami met through FJ1 and whom he was initially going to marry. However, the difference in their views on Islam (Hammami identified to Salafism, FR5 to Sufism) changed the course of Hammami's life. Hammami refused marriage with FR5, which he claims allowed him to devote more time to his Islamic studies and delve deeper into his Islamic-based ideologies on Salafi Islam and jihad. FJ1 also influenced Hammami to move to Toronto to escape the religious persecution of the small town of Daphne. It was in Toronto that Hammami connected with the Somali-Canadian community, where he began to learn about the persecution of Somali Muslims at the hands of the Christians in neighboring Kenya; this deepened his feelings for jihad. FJ1 was the only friend who practiced Islam and prayed with Hammami during their time in high school. FJ1 also introduced Hammami to his

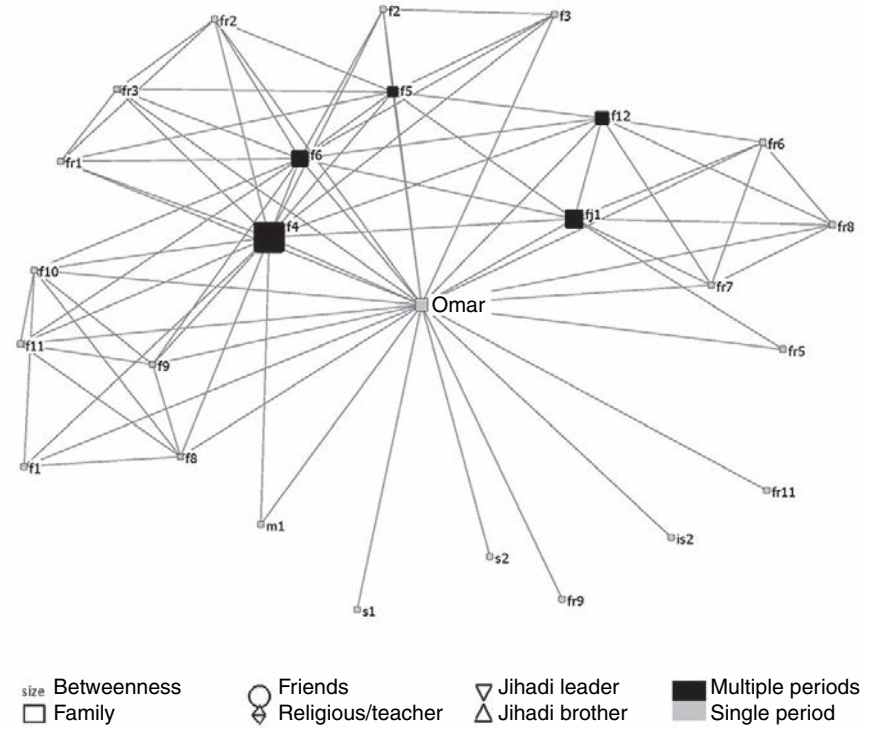


Figure 5.2 Hammami's pre-jihad network in Daphne, USA, and Toronto, Canada.

first wife, F12, who was a Somali–Canadian. F12 became pregnant with Hammami's first child while living in Toronto and together, as a group, FJ1, Hammami and their families made plans to move to Alexandria, Egypt, to continue their journey.

It was in Alexandria that the true transition to becoming radicalized occured for Hammami. Figure 5.3 presents Hammami's network in Alexandria (bottom of Figure 5.3) and the network in which he immersed himself into in the next phase of his journey in Mogadishu, Somalia (top of Figure 5.3). As mentioned, many of the family and friends he had in Toronto followed him to Egypt, including FJ1 and Hammami's wife F12. Two key actors emerged in this network, actors who were important in Hammami's transition to become a homegrown terrorist. The first was FR10 (middle of the cluster at the bottom of the diagram), the father of Hammami's Egyptian friend F9 whom he met while living in Toronto. FR10 allowed him to remain in Egypt after FJ1 and family, as well as Hammami's wife and child, moved back to the United States. FR10 offered Hammami a place to stay and provided him with connections to local Muslim shaykhs, Muslim teachers and local mosques. The move to Alexandria would ultimately lead to Hammami meeting FJ2 (middle of the cluster, right side of the diagram), who became both his best friend and his jihadi brother and with whom he later moved to Somalia. FJ2 introduced

Hammami to radical Muslim scholars and it was only after this that he declared having become a jihadi (Hammami, 2012: p. 34).

Both Hammami and FJ2 moved to Mogadishu together and integrated a network almost exclusively composed of jihadi bothers and leaders (right side of Figure 5.4). Importantly, though this visit was the first for Hammami, FJ2 had traveled before to Somalia and made contacts with individuals belonging to Al-Shabaab. It was FJ2 who introduced Hammami to several jihadi brothers (J1, J2, J3 and J4) who were members of Al-Shabaab when Hammami first arrived in Mogadishu. Hammami would eventually accompany these jihadi brothers on the road to Kismayu, where he would meet leaders of Al-Shabaab. These five central players were all influential as catalysts from radicalization to violence in Hammami's journey to jihad. This was the difference between Hammami having simply radicalized and him being involved in terrorist missions. Important to note is that before the next phase of Hammami's journey (Chiamboni, Somalia), FJ2 left the group due to sickness. FJ2 and Hammami did not see each other again during the time frame represented in the autobiography.

As can be seen in Figure 5.4, which shows Hammami's network at three time periods in Somalia, the departure of FJ2 left Hammami with no ties to his former life once he arrived in Chiamboni, Somalia. This is where Hammami met with JL6

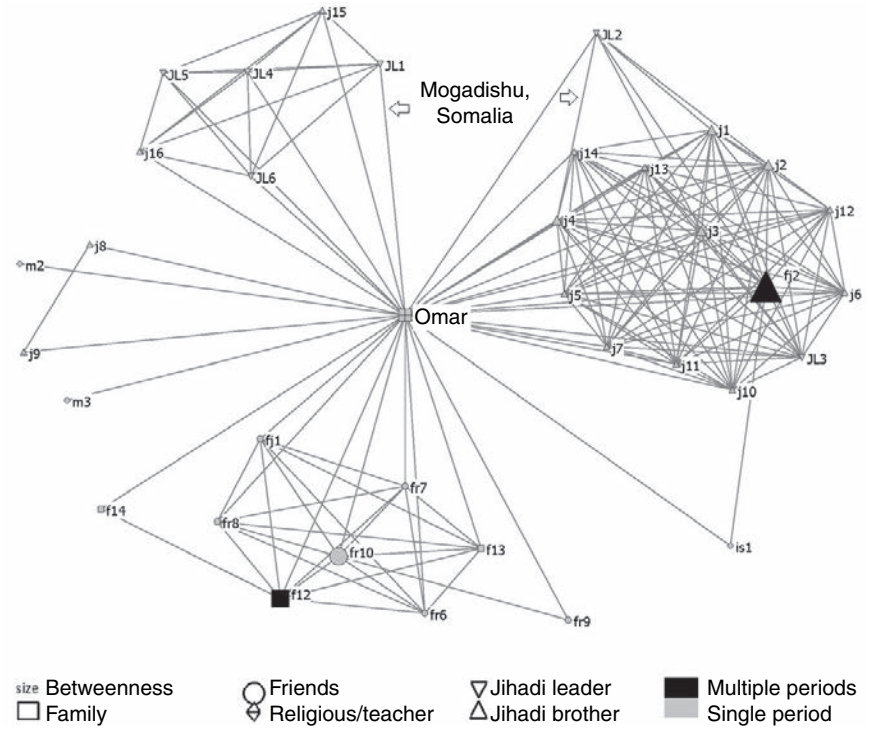


Figure 5.3 Hammami's network in Alexandria, Egypt, and Mogadishu, Somalia.

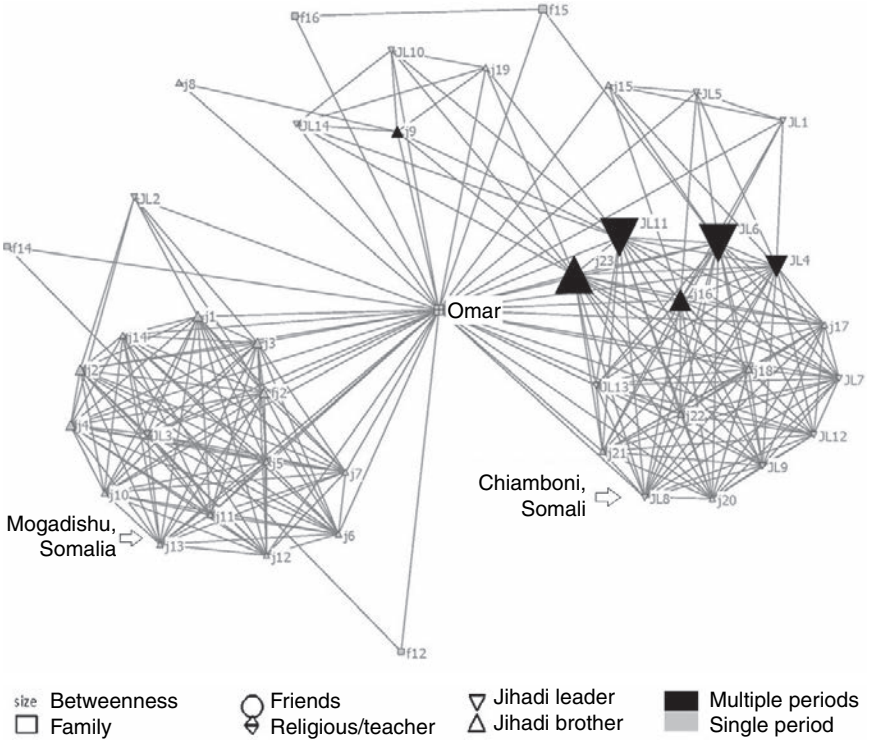


Figure 5.4 Hammami's Somalia network—three cities combined.

(middle right side of the network), who was the alleged leader of the Al-Shabaab terrorist network[4] (Dagne, 2011). Actor JL6 was in a structurally influential position in Hammami's network, bridging the time period from Mogadishu, the beginning of Hammami's journey in the Somali network, to the Chiamboni network where Hammami learned advanced training techniques in fighting and weapons use. JL6 also connected Hammami with J16 (middle of Chiamboni network), who owned Al-Shabaab's headquarters, and to Hammami's second wife (F15), who bore his first son (F16, both at the top of the network). Chiamboni brought Hammami deeper into isolation from family and friends, including F15 (his current wife), his newborn son (F16) and his family in the United States.

It is during this time period (February 2010) that the split between Hizbul Islam (Asmara group) and the Xarakah ash-Shabaab al-Mujaahidiin (new Al-Shabaab) occured (Dagne, 2011). Here, Hammami was faced with a crossroads at which time he could have chosen a less militant path by following the Asmara group. However, his strong ties to JL6, as well as to J9 whom Hammami had known since Mogadishu and who would become the leader of Xarakah ash-Shabaab al-Mujaahidiin, led him to choose a more violent path. After the split,

Hammami traveled to Baraawe to continue his personal jihad. The Baraawe network (upper middle of the diagram) was much smaller and included six contacts (J9, J19, J23, JL10, JL11 and JL14). This network structure coincided with Hammami's description of Xarakah ash-Shabaab al-Mujaahidiin as being an extremely small camp after the split. The Baraawe network was completely homogeneous, made up of individuals who all shared the same socio-political ideologies and extremist views about Islam, jihad, and the future direction of Al-Shabaab. In network analysis, this is known as a clique.

The network attrition which started when Hammami left Egypt and reached a peak in Baraawe is consistent with the literature on the radicalization of homegrown terrorists, describing that part of the process of radicalization when individuals isolate themselves and surround themselves with like-minded others (Beutel, 2007; Gartenstein-Ross and Grossman, 2009; Horgan, 2003; Wiktorowicz, 2004; Wilner and Dubouloz, 2010). The complete isolation of Hammami and his small group of militants at this point may have been a precursor to his eventual murder in September 2013. Angering the leaders of the Asmara group (the less militant arm of Al-Shabaab after the split) and having no peripheral social ties on which to call upon, Hammami may have sealed his own fate.

There are two final observations to make about the evolution of Hammami's network. First, his network gradually shrank after he left Mogadishu and became more deeply involved with members of Al-Shabaab. This dynamic is illustrated in Figure 5.5, which follows Hammami's network density and network size as he moved from one location to the next. Starting in Chiamboni, he made contact with more highly influential members of Al-Shabaab, establishing stronger ties

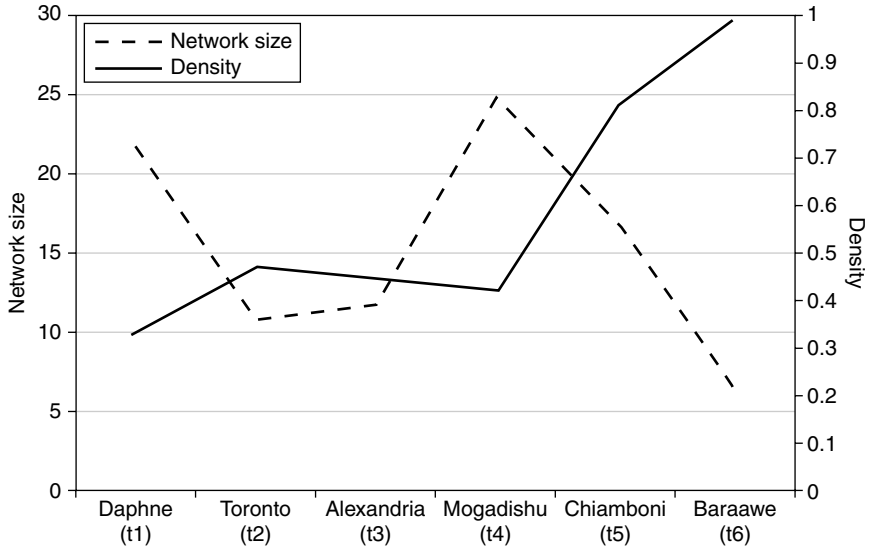


Figure 5.5 Hammami's network density by time period and location.

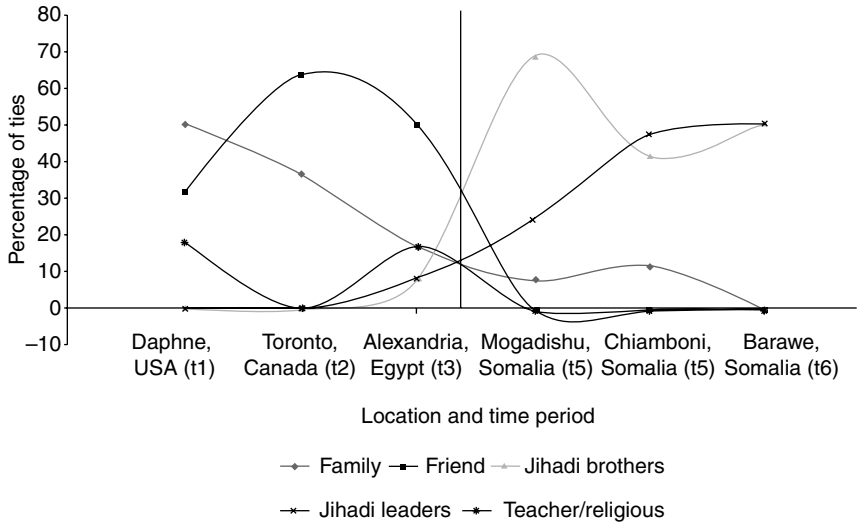


Figure 5.6 The proportion of ties in Hammami's network by time period and location.

within groups who shared the same Islamic extremist ideologies until he finally isolated himself among a very small, trusted, perfectly cohesive group of individuals after travelling to Baraawe.

Second, examining the nature of the ties in Hammami's network at different time periods allows us to better appreciate the timing of the transition that occurred in his radicalization trajectory. Figure 5.6 shows the proportion of ties for each type by time period. The figure shows a clear transition from Hammami's family and friends to a complete integration within jihadi networks in Somalia. The transition occurs in Egypt (t3) when Hammami first encountered a jihadi brother, who became his best friend (FJ2), and was encouraged by two individuals he identifies as Salafi Qur'an teachers (M2 and M3) to continue to move to Somalia to engage in his personal jihad with Al-Shabaab. At this point the proportion of family members and pre-jihad friends in his network were decreasing quickly, reaching new lows in time 4 when Hammami arrived in Mogadishu, Somalia. The only two family members remaining in the network at this point were his wife (F12) and her grandmother (F14). An almost complete overhaul in his friendships occurred in Mogadishu, when 92 percent of his network was made of jihadi brothers (68 percent) and leaders (24 percent). He used the rest of his time in Somalia to move closer to the Al-Shabaab leadership and eventually trim his network to only six contacts in Baraawe (t6).

Conclusion

This study provides an individual perspective of the radicalization process of a homegrown terrorist from the United States through the application of social

network analysis. By examining the structure of Omar Hammami's personal network through time, we were able to identify specific turning points and influential individuals important in his radicalization process to becoming a homegrown terrorist. This study joins other scholars who increasingly argue for using network analysis to understand the radicalization process and the formation of terrorist groups (Everton, 2012; Helfstein, 2012; Sageman, 2004, 2008; Southers, 2013). The majority of those who engage in extremist ideologies do not cross over to commit violent acts in the name of their extremist views (e.g., Southers, 2013). As Huey and colleagues (this volume) and many others before them remind us, many radicalization trajectories are not linear and predictable. Most trajectories of radicalization never lead to actual acts of violence.

The present study also offers evidence that exposure to radical or extremist ideologies, alone, may not explain why an individual becomes radicalized when others who are similarly exposed do not. Hammami's early exposure to two religious traditions contributed to a desire to learn more about religion generally, before the encounter with influential Salafi teachers oriented his journey towards an extremist view of Islam. The support he found in these views from his close friends, and his sensitivity to issues touching the Somalian community, kept Hammami focused on a quest to become "a pure Muslim."

Case studies such as Hammami's are useful to illustrate many aspects of the radicalization process but are also subject to several limitations that are worth stating here. The first limitation of this study concerns the issue of boundary specification. Social networks, particularly illegal networks in which the goal of members is to remain undetected, pose problems for missing data resulting in omission errors of missing nodes or edges (actors and their ties) or errors in attribute specification of nodes and edges (Borgatti *et al*., 2013). In Hammami's case we rely mostly on the contacts that he chose to discuss in his book, which leads to a second, related limitation of the study. The use of secondary sources allowed us to alleviate some of the omissions of the book, and to cross-check the validity of many details found in the book. We note, however, that the issue of missing network data may be less serious in this case where the objective is to identify key individuals in Hammami's radicalization process, as opposed to a different study that would have aimed at mapping the social structure of the Al-Shabaab network. In the latter case, the view of a single individual over an entire organization is bound to be severely truncated.

Despite these limitations, we hope that this case study focusing on Hammami's network will continue to foster reflection regarding the programs that support Muslim youth who may be at risk of following a similar pathway. Mapping the social networks around these extremist individuals helps us identify the timing of changes in radicalization processes and the effect of these changes on their relationships at key moments in their lives. This kind of analysis, however, does not provide any suggestion as to what exactly would help individuals change their views to less radical ones. But it does naturally lead to the suggestion that if social ties are so critical to the process of radicalization, then social ties may be similarly important to reversing this process.

Notes

1 Although Hammami often uses real names in his book, we decided not to use any for the purpose of this chapter. Despite the use of secondary data sources to supplement the material which largely converged with Hammami's account, most of our data come from his book and we are careful not to repeat any errors in attribution that may have existed in the original source. We are interested in social network patterns in his radicalization trajectory and focus on these instead of on the names of individuals reported in his book and elsewhere.
2 "Salafi" is the Islamic term for a modern follower of Sunni Islam in which a literal and strict adherence to the Qur'an is called for; the Salafi movement is often considered to be extremist (Livesey, 2005).
3 Although every one of the 71 contacts extracted were classified in one of these five categories, the labels we used to identify each contact allowed us to specify differential status within a category. For example, one of Hammami's religious influences was an online contact labeled IS1 for "Internet source." Another Internet source labeled IS2 was a highly ranked Al-Shabaab recruiter and was coded as a jihadi leader. Importantly, two of Hammami's best friends were labeled as FJ1 and FJ2 (or "friend and jihad brother") and coded as "friend" and "jihad brother" respectively. The former was coded as "friend" because the friendship developed in high school before any of them started their radicalization process. The latter was coded as "jihad brother" because the friendship developed in the context of Hammami's early radicalization process and led to his introduction to Al-Shabaab members.
4 JL6 was designated on 3 June 2004 as a foreign person who is eligible for sanctions under US Executive Order 13224 in which the primary purpose is to block property and prohibit transactions of persons who commit, threaten to commit, or support terrorism (US Department of the Treasury, 2000).

References

Bakker, E. (2006) *Jihadi Terrorists in Europe, their Characteristics and the Circumstances in which they Joined the Jihad: An Exploratory Study*. The Hague: Netherland Institute of International Relations/Clingendael.

Beutel, A. J. (2007) Radicalization and homegrown terrorism in western Muslim communities: Lessons learned for America. *Minaret of Freedom Institute*.

Borgatti, S. P., Everett, M. G. and Freeman, L. C. (2002) *Ucinet 6 for Windows: Software for Social Network Analysis*. Cambridge MA: Analytic Technologies.

Borgatti, S., Everett, M. G. and Johnson, J. C. (eds) (2013) *Analyzing Social Networks*. Thousand Oaks CA: Sage Publications, Ltd.

British Broadcasting Corporation (BBC) (2009) Profile: Somalia's President Ahmed. 3 February.

British Broadcasting Corporation (BBC) (2013) Al-Amriki and al-Britani: Militants killed in Somalia. 12 September.

Brooks, R. (2011) Muslim "homegrown" terrorism in the United States: How serious is the threat? *International Security*. 36 (2), pp. 7–47.

Carley, K. M. (2007) *Dynamic Network Analysis in Counter-terrorism*. Pittsburgh: Carnegie Mellon University.

Crone, M. and Harrow, M. (2011) Homegrown terrorism in the West. *Terrorism and Political Violence.* 23 (4), pp. 521–536.

Dagne, T. (2011) Somalia: Current conditions and prospects for a lasting peace. Congressional Research Service Report for Congress, August.

Everton, S. (ed.) (2012) *Disrupting Dark Networks: Structural Analysis in the Social Sciences*. New York: Cambridge University Press.

FBI (Federal Bureau of Investigation) (2007) National press releases: FBI's top ten stories for the week of July 27, 2007. FBI National Press Office.

FBI (Federal Bureau of Investigation) (2012) Omar Shafik Hammami added to the FBI's most wanted terrorist list. FBI: Mobile Division.

Freeman, L. C. (1979) Centrality in social networks: I. Conceptual clarification. *Social Networks.* 1, pp. 215–239.

Gartenstein-Ross, D. and Grossman, L. (2009) *Homegrown Terrorists in the U.S. and U.K.: An Empirical Examination of the Radicalization Process*. Foundation for Defense of Democracies Center for Terrorism Research, Washington DC.

Hammami, O. (Mansuur al-Amriiki, Abu) (2012) *The story of an American jihaadi: Part one*. May 2012. Available at: www.scribd.com/doc/93732117/The-Story-of-an-American-Jihaadi and http://azelin.files.wordpress.com/2012/05/omar-hammami-abc5ab-mane1b9a3c5abr-al-amrc4abkc4ab-22the-story-of-an-american-jihc481dc4ab-part-122.pdf. Accessed 6 June 2012.

Hegghammer, T. (2006) Terrorism recruitment and radicalization in Saudi Arabia. *Middle East Policy.* 8 (4), pp. 39–60.

Helfstein, S. (2012) Edges of radicalization: Ideas, individuals and networks in violent extremism. Combating Terrorism Center, West Point.

Horgan, J. (2003) The search for the terrorist personality. In Silke, A. (ed.) *Terrorists, Victims and Society: Psychological Perspectives on Terrorism and its Consequences*. Chichester: John Wiley and Sons, pp. 1–28.

Jenkins, B. M. (2009) Outside expert's view. In Gartenstein-Ross, D and Gorssman, L. *Homegrown Terrorists in the U.S. and U.K.: An Empirical Examination of the Radicalization Process.* Washington DC: Foundation for Defense of Democracies.

Jenkins, B. M. (2011) Stray dogs and virtual armies: Radicalization and recruitment to jihadist terrorism in the United States since 9/11. Rand Corporation.

Koschade, S. (2006) A social network analysis of Jemaah Islamiyah: The applications to counter-terrorism and intelligence. *Studies in Conflict and Terrorism.* 29 (6), pp. 559–575.

Krebs, V. E. (2002) Mapping networks of terrorist cells. *Connections.* 24 (3), pp. 43–52.

Krueger, A. B. (2008) What makes a homegrown terrorist? Human capital and participation in domestic Islamic terrorist groups in the U.S.A. *Economic Letters.* 101 (3), pp. 293–296.

Livesey, B. (2005) The Salafist movement: An examination of the ideology that has inspired the global jihad and the emergence of its most dangerous incarnation. *Frontline*, Public Broadcasting Service.

McCants, W., Brachman, J. and Felter, J. (2006) *Militant Ideology Atlas*. Combating Terrorism Center, U.S. Military Academy.

Mohamed, M. (2012) Hizbul Islam's split from al-Shabaab further isolates militant group. *Sabahi*. 27 September.

Morselli, C. (2001) Structuring Mr. Nice: Entrepreneurial opportunities and brokerage positioning in the cannabis trade. *Crime, Law and Social Change.* 35, pp. 203–244.

Morselli, C. (2003) Career opportunities and network-based privileges in the Cosa Nostra. Crime, Law and Social Change. 39, pp. 383–418.

Morselli, C. (2009) *Inside Criminal Networks*. New York: Springer.

Powers, S. M. (2014) Conceptualizing radicalization in a market for loyalties. *Media, War and Conflict.* 7 (2), pp. 233–249.

Precht, T. (2007) Home grown terrorism and Islamist radicalisation in Europe—from conversion to terrorism. In *Research report Funded by the Danish Ministry of Justice*. Copenhagen: Danish Ministry of Justice.

Rodriguez, J. A. (2005) The March 11th terrorist network: In its weakness lies its strength. Paper presented at the 8th Congreso Español de Sociología, Alicante.

Sageman, M. (ed.) (2004) *Understanding Terror Networks*. Philadelphia: University of Pennsylvania Press.

Sageman, M. (ed.) (2008) *Leaderless Jihad: Terror Networks in the Twenty-First Century*. Philadelphia: University of Pennsylvania Press.

Southers, E. (ed.) (2013) *Homegrown Violent Extremism*. Waltham MA: Anderson Publishing.

Toth, N., Gulyás, L., Legendi, R. O., Duijn, P., Sloot, P. M. A. and Kampis, G. (2013) The importance of centralities in dark network value chains. *The European Physical Journal Special Topics.* 222, pp. 1413–1439.

U.S. Department of the Treasury (2000) Terrorism: What you need to know about U.S. sanctions. Office of Foreign Assets Control.

Wiktorowicz, Q. (2004) Joining the cause: Al-Muhajiroun and radical Islam. Paper presented at The Roots of Islamic Radicalism Conference, Yale University, 8–9 May.

Wilner, A. S. and Dubouloz, C. J. (2010) Homegrown terrorism and transformation learning: An interdisciplinary approach to understanding radicalization. *Global Change, Peace and Security.* 22 (1), pp. 33–51.

Xu, J., Hu, D. and Chen, H. (2009) The dynamics of terrorist networks: Understanding the survival mechanisms of global Salafi jihad. *Journal of Homeland Security and Emergency Management.* 6, pp. 1–33.

6 A radical sociability

In defense of an online/offline multidimensional approach to radicalization

Benjamin Ducol

Introduction

In recent years, terrorism[1] and violent radicalization have become an issue of top concern for public authorities both in Europe and North America. Meanwhile, the rapidly changing nature of the threat has severely complicated the common understanding of clandestine political violence and the ways governments and societies can prevent and respond to its offshoots. At the center of attention, the Internet[2] has been pointed to by many as a new crucial element to be taken into account in the equation. As expressed by Rob Wainwright, director of Europol: "terrorism continues to evolve from structured groups and networks to smaller groups and solo terrorists or lone actors, while the Internet remains a key facilitator for terrorism-related activities" (TE-SAT, 2013, p. 14).

The Internet is part of the daily life of most people, and violent extremists are no exception. Indeed, political extremists around the world have been quick to embrace the potential of digital networks with particular enthusiasm and vigor. While the Internet has become a worldwide platform for communication, radical militants have never ceased their attempts to leverage the power of cyberspace in a myriad of ways, ranging from propaganda uses to more concrete operational matters (Weimann, 2006a; Conway, 2006; Awan, 2007). Commentators' use of catchwords such as the "web of terror," the upsurge of an "Internet jihad" or the ascent of an "online terror underworld" encapsulate the importance that the Internet has taken on in current terrorism trends.

This chapter is intended to address, from a theoretical point of view, the complex relationship between the Internet, processes of radicalization and individual trajectories towards terrorism. After introducing current debates and providing a critical overview of the growing body of literature available on this topic, I will turn to a closer examination of the current pitfalls in the field that need to be overcome if we truly aim to shed light on the Internet's significance in regard to radicalization processes and pathways towards clandestine political violence. A comprehensive understanding of radicalization phenomena must surely take into consideration how virtual environments impact—or not—the emergence of socializing settings and practices through which people come to adopt belief systems and cognitive frames that embrace political violence as a

legitimate avenue of action and that might, in certain conditions, lead them to actively engage in some form of "terrorist career."[3] Accordingly, the next section in this chapter will discuss the need to recast our conceptualization of radicalization in order to better integrate the role of online settings that can expose individuals to a wide range of radicalizing influences. Drawing on Situational Action Theory (SAT), this chapter will demonstrate the importance of focusing on the relational setting—the radical sociability—through which some individuals come to acquire a propensity to perceive involvement in terrorism-related activities as a legitimate action alternative. At the same time, I assert that it is equally important to examine online and offline life-spheres in which people are embedded, as they simultaneously contribute to shape the development of cognitive configurations supporting political violence. In sum, my approach attempts to grasp the impact that both online and offline life-spheres can have on behavioral outcomes and pathways towards terrorism, neglecting neither the importance of real world interactions nor the influence of cyberspace dynamics.

Political violence and terrorism in the digital era: the sum of all fears?

A detailed account of the convergence of the Internet and contemporary terrorism is beyond the scope of this chapter and is still to be written. Nevertheless, it seems obvious to note that digital networks have altered the way modern terrorism can be understood. Over the last decade, cyberspace has been characterized by a mass proliferation of extremist content and terrorism advocacy websites. Notwithstanding the difficulty of precisely quantifying this phenomenon (Ramsay, 2013), it appears clear that the Internet has become an additional space for political extremists, regardless of ideological agenda or geographical location, to present their case and openly advocate political violence at very low technical and human cost. It is no surprise that radical militant groups all over the world and their armchair supporters have become increasingly comfortable operating online, where they have long established a multidimensional presence (Seib and Janbek, 2010). Modern media ecology has facilitated the broad diffusion of extremist narratives beyond national frontiers, and by the same token has helped terrorist organizations publicize their actions outside of a strictly local framework (Campana and Ducol, 2015). On one hand, the web has made it easier for radical militants to reach new audiences and to mobilize potential supporters across physical borders. On the other hand, the advent of digital networks has had immediate consequences for ordinary web users in the "real world," lowering barriers to accessing extremist online propaganda. Consuming extremist media content and accessing websites openly advocating terrorism has never been easier in history.

This phenomenon has been accelerated as a result of recent changes in the Internet landscape. The democratization of mobile Internet access around the world and the takeoff of Web 2.0 in the mid-2000s have led to a more

user-centric online environment. While in the past, terrorist groups were able to maintain a strong level of control over their presence in cyberspace, the emergence of Web 2.0 has radically altered the face of extremist virtual presences (Weimann, 2010; Conway, 2012). Political extremism on the Internet extends far beyond official websites directly operated by terrorist organizations. Present-day radical militant groups are merely the primary actors of their online footprint. They rely on a crowd of anonymous sympathizers and wannabe extremists who are collectively engaged in the virtual dissemination of narratives and media content supporting the cause. Fan websites and unofficial online voices act as free publicity for many political extremist movements, which can rely on this uprooted network of armchair supporters to echo their claims in cyberspace (Amble, 2012).

All of these inherent challenges posed by the confluence of digital networks and clandestine political violence phenomena have led governments to become increasingly concerned with the extended role that the Internet has taken on in the current terrorism context. Policy-makers and security officials have been particularly worried about the role that digital networks might play as key facilitators for involvement in terrorism-related activities. Today, terrorism cases without a "digital footprint" are becoming increasingly rare. As rightly noticed by King and Taylor (2011), "The Internet has featured one way or another in each homegrown jihadi terrorist plot since 2002" (p. 618). This pattern has been extensively confirmed during field interviews conducted with professionals—anti-terrorist police officials and judges—involved in the prevention and suppression of terrorism activities, both in Europe and in North America.[4]

While the Internet appears to be a recurring piece of the puzzle in terrorism investigations, academics working in the field of terrorism studies have not been idle in trying to clarify the potential function that the Internet might have in processes of radicalization. In recent years, a substantial body of research has been devoted to these issues with some progress, but also many pitfalls. Myths and popular beliefs surrounding the role played by the Internet as a tool of radicalization have proliferated in the news and sometimes in academia (Hoskins and O'Loughlin, 2009), with little empirical evidence to inform a comprehensive understanding of this phenomenon (Edwards and Gribbon, 2013). As rightly captured by Conway (2012): "There is an assumption that the Internet plays a part in some individuals' radicalisation, on the basis of self-reporting, but not large-scale studies showing this to actually be the case or measuring the extent of the Internet's role in such process" (p. 13). What role does the Internet specifically play in regard to current terrorism trends? Does cyberspace act as an environment for fostering radicalization processes? Are digital networks increasing the opportunities for incremental involvement into terrorism-related activities? Is the Internet merely a source of inspiration for wannabe radicals or a true facilitator for self-radicalization and self-engagement into clandestine political violence? All of these questions remain unresolved and without doubt need further investigation from scholars and experts.

Terrorism's digital footprint: what do we know and what don't we know?

Overall, the current literature concerned with political violence and terrorism phenomena in the digital era[5] can be categorized into four distinct subject areas.[6] The first area incorporates studies that are primarily concerned with how extremists and terrorist organizations leverage cyberspace to undertake operational activities including online training, planning and logistics for future attacks (Thomas, 2003; Weimann, 2005). With the global accessibility of the new media environment, the temptation has been high for practitioners and academics to perceive cyberspace as a new kind of "safe haven" for terrorist activities (Ranstorp, 2007; Judy, 2011). So far, such publications have described in more or less detail the range of instrumental uses terrorist organizations make of digital networks, such as recruitment (Kohlmann, 2008; Torok, 2010), financing (Jacobson, 2010), training (Weimann, 2006b; Stenersen 2008, 2013) and operational planning (Gohel, 2009). Such instrumental uses of the Internet by terrorists surely exist, but they appear overall to be a marginal phenomenon. Empirical evidence does not support the conclusion that digital networks have been widely used as a base of operations by radical militant groups. Many researchers acknowledge that a strong focus on cyberspace as a reliable source of operational purposes for terrorism is misplaced (e.g., Kenney, 2010; Ramsay, 2013; Benson, 2014). In response, another body of research has emerged, emphasizing the importance of going beyond the biased examination of strictly instrumental uses of digital networks for terrorism purposes to the examination of its communicational components.

This second subject area focuses on the communicational dimensions of cyberspace. It looks at the propagandist uses of the Internet by terrorist organizations and how extremists have embraced the online mediascape to promote their cause and disseminate their ideology (Conway, 2006). Many studies examine the way extremists in the post 9/11 era leverage virtual opportunities to establish a pervasive online presence (Seib and Janbek, 2010). Privileged topics such as the framing strategies developed by extremist movements such as Hamas (Mozes and Weimann, 2010), Hezbollah (Weimann, 2008b) and Irish Republican paramilitary organizations (Bowman-Grieve, 2010; Reilly, 2011; Bowman-Grieve and Conway, 2012) have been a subject of high interest for scholars. Yet global jihadism has until now attracted most of the attention with regard to this branch of knowledge. Academics have described the scope and the role of digital networks within the global jihadi movement (Rogan, 2006, 2007; Lia, 2006; Torres-Soriano, Jordán and Horsburgh, 2006; Kimmage, 2008, 2010). At the macro level, particular attention has been paid to the history of online jihadi media including Al-Qaeda's digital tools (Brachman, 2009; El Difraoui, 2013) and its media strategies (Ciovacco, 2009). The growth of virtual media production and distribution entities linked to various groups operating under the general ideological rubric of the global jihadi movement has also been an important topic of interest among researchers (Torres-Soriano, 2010).

Increasingly, scholars are interested in capturing the evolution and the dynamics of the jihadi media ecosystem. Some authors provide descriptive analyses of online jihadi media entities (Kimmage 2008; Weimann 2008a) such as the Global Islamic Media Front, also known as GIMF (Torres-Soriano, 2012), while others are engaged in a more comprehensive analysis of jihadi forums and their *raison d'être* (Kohlmann, 2010; Ducol, 2012; Zelin, 2013; Torres-Soriano, 2013). Another subfield is engaged in the task of mapping the scope of jihadi presence online using a wide set of mixed methods including computational data mining, network analysis and online cartography (Reid and Chen, 2007; Chen *et al*., 2008; Chen, 2011; Klausen *et al*., 2012; Campana and Ducol, 2014). Identical procedures have also been applied to violent extreme-right groups in Europe and North America with several interesting developments (Burris *et al*., 2000; Tateo, 2005; Caiani and Wagemann, 2009; Sutton and Wright, 2009; Caiani *et al*., 2012). Overall, these studies are useful in assessing the scope of extremist presence online and the varied forms it takes, but they do not help much in understanding the precise role of the Internet in pathways towards terrorism.

A third subject area is more specifically attentive to the "supply side" of extremist digital content—digital publications, videos, etc.—and how they are distributed throughout the web. Seeing the Internet as an "invisible hand" that organizes terrorist activities worldwide, academics have aimed to describe what kind of material is disseminated online, for which purposes, and how anonymous users collectively participate in the production of discourses, narratives and visual motifs that strengthen and promote already existing extremist frames[7] (Archetti, 2012). Scholars around the world have engaged with various elements of these cyberdynamics and investigated how political extremists and their armchair supporters are interactively shaping the frontiers of ongoing radical countercultures in cyberspace (Tsfati and Weimann, 2002). Online jihadism (Egerton, 2011; Lohlker 2013a, 2013b; Ramsay, 2013) as well as oppositional extreme-right and white supremacist digital subcultures (Back, Keith and Solomos, 1998; Duffy, 2003; Gerstenfeld *et al.*, 2003; Roversi, 2008) have been the subject of extensive research throughout the years. Many studies have examined the symbolic realities and "rhetorical visions" (Bormann, 1972) used by political extremists in cyberspace and how these elements contribute to the shaping of radical world views by using ideologically crafted fantasy themes and visual motifs (Fighel, 2007). Shared rhetorical visions, discourses and visual motifs sustain what Bolt refers to as an "archipelago of memory" (Bolt, 2012), in other words the crafting of an uprooted political imaginary that reinforces a shared sense of belonging to a common "imagined community" (Silke, 2010, p. 34; Egerton, 2011, p. 92).

Interactive features of modern web-based technologies have facilitated a broader dissemination of autonomous user-generated cybercontent outside official websites and digital platforms. In parallel, it has also eased the emergence of undefined online communities, radical digital milieus (Conway, 2012), that encompass a wide cross-section of producers and consumers who all contribute to the everyday re-making and dissemination of extremist narratives through

cyberspace. The role of these extremist virtual communities (Janbek and Prado, 2013) in fostering a sense of shared identity and mutual commitment has begun to be explored by several scholars (De Koster and Houtman, 2008; Bowman-Grieve, 2009; Bowman-Grieve and Conway, 2012). In many cases, online interactions within extremist online communities and between their members are alleged to validate the existence of stable online communities of related users united by a shared political imaginary (O'Callaghan *et al*., 2012). In return, authors including Conway rightly raise the question of "the ability of [these] online radical milieus to produce 'real world' terrorists" (Conway, 2012, p. 17). With recent changes observed in the virtual mediascape, social media is by some means extending the traditional frontiers of these radical online milieus by blending in social media platforms such as YouTube, Twitter and Facebook (Weimann, 2010). Some researchers go so far as to consider that three-dimensional virtual communities such as Second Life might potentially act as permissive environment for radicalization (Cole, 2012). Problematically, many of these studies tend to equate any individual participation to these extremist online communities as a predicting factor for radical behavior outcomes in the "real world."

Finally, a fourth group of studies is concerned with the impact of extremist media content on people, both online and offline. Scholars are interested in determining if the consumption of extremist material by individuals and their frequent exposure to online radical milieus can explain, to some extent, radicalization processes and further involvement in clandestine political violence. Almost all recent studies about terrorism and political violence make mention of the Internet as a key facilitator in promoting radicalization (Precht, 2007; Dalgaard-Nielsen, 2010; King and Taylor, 2011). Though many of them suggest that digital networks play a role in radicalization processes either as a driver or reinforcing mechanism (Sageman 2004, 2008; Silber and Bhatt, 2007; Köhler, 2012), few go further into detailing how these processes concretely happen. The hypothesis that cyberspace has a significant role in the process of radicalization appears to be based on the problematic premise of a natural causal link between the wide availability of extremist content in cyberspace on one hand, and on the other, anecdotal cases of individuals engaged in terrorism who had previously been exposed to extremist media content (Gartenstein-Ross and Grossman, 2009; Homeland Security Institute, 2009; Briggs and Strugnell, 2011). In sum, this biased assumption assumes a "magic bullet" association between the Internet and the processes of radicalization, rather than a careful examination of the reality of this causation and its specific mechanisms.

So far, very little is known about how individuals experience and react to the consumption of extremist materials found online or about what influence it has on them, in either the short or the long term (Lennings *et al*., 2009; Edwards and Gribbon, 2013). To date, studies focusing on the Internet and prospects of radicalization have assumed a natural link between extremist cybercontent and its influence on individuals in the "real world." In consequence, scholars tend to disagree over the extent to which online content is able to radicalize and

transform individuals into supporters of—or active participants in—violent political actions. While a number of studies have attempted to describe the varied contours of the role of digital networks in radicalization, it remains extremely difficult to ascertain it. Few researchers have tried to examine how online social dynamics might influence radicalization patterns in cyberspace, and even these researchers have not provided strong conclusions to support the tangibility of such phenomena. For example, Conway and McInerney (2008) have attempted to explore virtual interactions among YouTube users in order to see if interpersonal dynamics across this video-sharing platform might open avenues for online radicalization. Other studies have mobilized a sentiment analysis framework to complement such social network analyses, but these studies have failed to deliver concrete evidence supporting the existence of such online radicalization processes (Chen, 2008; Bermingham *et al*., 2009).

Beyond the pitfalls of current studies about the Internet and radicalization

Does extremist online content available through cyberspace play a substantial role in the process of radicalization? In light of the previous discussion, it appears clear that there is a knowledge gap in our understanding of how the Internet might insert itself into varied trajectories of involvement into clandestine political violence. Until now, scholars studying the issue of Internet radicalization have been focusing their attention on the "supply side" of political extremist material, leaving outside the picture the question of how individuals might engage with extremist settings widely available on the Internet and whether they experience them on a regular or inconsistent basis. To date, academics have neglected to interrogate how users' peregrinations in cyberspace precisely influence their pathways towards terrorism in the "real world" and vice versa. If the Internet does indeed have a role in the process of radicalization, the next challenge for scholars and policy-makers is to assess how the Internet can have such an effect. At the same time, a critical review of the current literature available reveals many issues that need to be addressed if future research is intended to unearth the mechanisms of Internet radicalization.

First and foremost, empirical evidence that the Internet plays a major role in facilitating radicalization and further commitment to clandestine political violence is currently far from being conclusive. Current understanding appears to be deeply limited by weak research methods, including an over-reliance on anecdotal evidence and secondary sources (Edwards and Gribbon, 2013). The lack of primary data is not exclusive to this particular subject area, but is often pointed out as the Achilles' heel of terrorism studies (Dolnik, 2013; Schuurman and Eijkman, 2013). For many reasons, notably the secretive, clandestine and violent nature of terrorism, collecting first-hand evidence can be quite difficult and is not without costs for academics engaged in fieldwork and empirical data collection. With few exceptions,[8] studies on the significance of digital networks in the process of radicalization do not rely on first-hand data collection. This

overwhelming dependence on secondary sources such as news and institutional reports has become highly problematic when exploring the Internet's impact on radicalization dynamics. It makes it difficult to distinguish between empirically tested hypotheses and merely speculated explanations that tend to proliferate in the contemporary literature on radicalization (Neumann and Kleinmann, 2013). Conducting primary research appears to be essential in order to gain a finer picture of how digital networks might influence individuals in their pathways towards political violence and terrorism commitment.

Another pitfall in the current literature is the epistemological bias driving many studies on Internet radicalization. Too often, authors uncritically assume a functionalist bias in presuming a strong causality between the exposure to extremist cybercontent and the effects that this content produces on people who are consuming it. This "hypodermic needle approach" of cyberspace echoes the direct effects theory in the field of media studies (Neuman and Guggenheim, 2011). The assumption that all Internet users might react uniformly when exposed to radical material is highly problematic and unrealistic. This assumption dubiously hypothesizes that individuals cannot escape from online extremist influences. Moreover, this functionalist bias does not help us gain a clearer understanding of why among a large number of individuals accessing terrorist websites and consuming all kinds of radical cybercontent, only a small minority will finally become radicalized and under certain conditions will engage in clandestine political violence. Because scholars and policy-makers have long focused their attention on the "supply side" of online political extremism, they tend to take for granted the idea that online extremist media content acts as an all-powerful force fostering radicalization processes in the "real world" (Briggs and Strugnell, 2011). Instead of asking "What does the Internet do to people?" we should in this case reverse this question and consider "What do people do with the Internet?"

In this line of argument, few studies have pushed to the foreground the notion of "self-radicalisation" linking the "growth of autodidactic extremists" (Pantucci, 2011) to the wide availability of extremist content in cyberspace. Accordingly, the Internet is often pictured as a powerful incubator of radicalization beliefs for lone extremist actors (Bjelopera, 2011). If the term self-radicalization is used to designate a person who came to be self-radicalized only through the Internet, these cases remain exceptional (RCMP, 2009, p. 10; Trévidic, 2013). As reflected by Neumann and Stevens (2009):

> Self-radicalisation and self-recruitment via the Internet with little or no relation to the outside world rarely happens, and there is no reason to suppose that this situation will change in the near future. The reason for the absence of self-radicalisation and self-recruitment online is that real-world social relationships continue to be pivotal.
>
> (Neumann and Stevens, 2009, p. 13)

It is difficult to imagine that mobilization through cyberspace would occur as easily as it can in the case of face-to-face configurations. In sum, the concept of

self-radicalization is essentially conjectural because it tends to treat the Internet as an autonomous life-sphere divorced from the social world reality.

The dichotomization of "virtual" versus "real world" is another major pitfall. In many cases, scholars tend to conceptualize virtual spaces as autonomous from what actually happens in the "real world" and vice versa. This epistemological stance proves to be problematic insofar as it revolves around a false dichotomy which artificially distinguishes cyberspace from the "real world." In reality, the Internet involves real people who cannot be considered outside of the socializing settings that constrain their beliefs and inform their guidance rules and daily actions in the "real world." In regard to radicalization processes in the digital era, it appears equally counterproductive to see the Internet as an all-powerful *deus ex machina* which would make all other factors irrelevant in our understanding of radicalization and pathways towards terrorism-related activities. The Internet represents only one piece of the radicalization puzzle. Future research should therefore pay closer attention to diachronic dynamics that can exist between online environments and "real world" social settings (Ducol, 2012). It cannot be assumed that there is a natural degree of causality between what happens online and the influence on individuals in the "real world." Instead, we need to recast the debate about online versus offline radicalization to reflect the fact that the two are less distinct than sometimes portrayed. To date, studies that have tried to capture the effects of both online and offline environments on radicalization processes are extremely rare (Wojcieszak, 2010; Warner, 2010; Von Behr *et al.* 2013).

Finally, there is a crucial need to establish an integrative theoretical framework from which it is possible to assess the Internet's influence on the radicalization process. The central matter is not whether the Internet has an influence on the radicalization process, but rather how we should think about it in the broader context of the production of knowledge on radicalization and terrorism. To fill this gap, we need first and foremost to rethink how digital networks can insert themselves into already existing theoretical frameworks about radicalization processes and terrorism. Many issues remain unexplored and the relationship between the Internet, radicalization processes and terrorism need to be recast in the light of further research. Why, if a large number of individuals consume online extremist content and visit terrorism websites, do only a small number of them in the end commit to political violence and potentially become involved in terrorism-related activities? Do settings and interactions in digital networks influence offline radicalization processes, and vice versa? Is the Internet acting as a "conveyor belt" or an "echo chamber"?

Recasting our understanding of radicalization: insights from Situational Action Theory (SAT)

As demonstrated in the previous section, the convergence of contemporary terrorism and the Internet remains, for the moment, a complex topic of study and an area of knowledge still to be explored. So far, the evaluation of the real significance of online environments in the process of radicalization and further

commitment to clandestine political violence has fallen short due to its reliance on anecdotal evidence and general assumptions and its tendency toward theoretical pitfalls. In recent years, many of these troubles have been amplified by the growing confusion surrounding the concept of radicalization and theoretical models that are supposed to explain the causal mechanisms behind this phenomenon (Neumann, 2013). Unfortunately, the assessment of the Internet as a key facilitator for radicalization cannot be divorced from the controversies surrounding what is exactly involved in this process and how we need to approach it. Determining whether digital networks play a crucial role in radicalization requires first reviewing what exactly is behind this process and how can it be useful to assess the impact of cyberspace as a fertile ground for mobilization and engagement towards clandestine political violence.

Trouble(s) with radicalization

Since the mid-2000s, the term radicalization has become a buzzword and a "catch-all concept" in the field of terrorism studies and counter-terrorism policy-making (Coolsaet, 2011). As is often pointed out in the academic literature, the notion of radicalization suffers from major issues and setbacks (Sedgwick, 2010; Richards, 2011). Among others, the lack of conceptual clarity and theoretical stretching have contributed to reinforcing several misunderstandings surrounding this all-inclusive concept. As noticed by Sedgwick (2010): "Radicalization is at present the standard term used to describe what goes on before the bomb goes off" (p. 479). Despite endless definitional controversies and the absence of an agreed definition (Pisoiu, 2013; Neumann, 2013), it would be highly counterproductive to discard this concept altogether (Schmid, 2013). Rather, radicalization needs to be more carefully defined and theorized in order to remain relevant in the study of political violence and terrorism.

Overall, radicalization is generally recognized among scholars as a gradual process of cognitive evolution towards certain beliefs, in some cases accompanied by corresponding behavior and attitude changes towards the acceptance of violence as a legitimate avenue of action (Moghadam, 2005; McCauley and Moskalenko, 2008; Mandel, 2009; Sinai, 2012). It is important here to highlight the fact that radicalization does not necessarily equate either with an actual involvement in political violence or with concrete acts of terrorism. Many authors draw distinctions between cognitive radicalization on one hand and violent political actions on the other (Taylor and Horgan, 2006; Bartlett *et al*., 2010; Borum, 2011a, 2011b). In consequence, radicalization and participation in terrorism-related activities cannot be treated as synonymous. A person can be radicalized, in the sense of morally supporting extremist ideas and acts of terrorism, but at the same time may never be concretely involved in the perpetration of violent political acts. This simple paradox shows that there is a crucial urge to disaggregate the concept of radicalization in order to make the distinction between the process of becoming cognitively radicalized and the process that results in an actual engagement towards acts of terrorism.

Radicalization through the lens of Situational Action Theory

In order to address these issues, it seems fruitful to turn towards Situational Action Theory (SAT) as developed by criminologist Per-Olof H. Wikström (2004). As we distinguish between the propensity to engage in clandestine political violence and the performance of actual acts of violence, the SAT allows us to recast our understanding of radicalization and terrorism. In brief, the SAT proposes that: "the convergence (in time and space) between a person's *propensity* and *exposure* initiates a *perception–choice process* whose outcome is an *action* or *inaction*" (Wikström *et al*., 2010, pp. 60–61). In this theoretical framework, actions are conceptualized as the result of individual's perceptions of their action alternatives and what action choices they make when confronted with the particularities of a setting (Wikström and Treiber, 2009). To summarize, the SAT focuses on how the intersection of individual cognitive schemes and social settings—*propensity* and *exposure*—produces a causal process—*a perception–choice process*—that brings about actions (see Figure 6.1). Applied to terrorism and political violence, the SAT allows us to refine what exactly is the process of radicalization and how to theoretically think about it.[9]

Using the SAT framework, radicalization can be defined as a situational process by which an individual acquires the propensity, and in some cases the intentionality, to engage in terrorism-related activities and acts of political violence (Bouhana and Wikström, 2011). This definition relies on the processual dimension of the SAT that regards radicalization as a perception–choice process. Inside this SAT framework, the transition from radicalization towards terrorism can be approached as a final, but not systematic, step in a radicalization process. It is important to conceptualize the process of radicalization as a necessary but not sufficient condition to enter a "terrorist career." As noted by Coolsaet (2011): "Terrorism is primarily the outcome of individual or small groups dynamics boosting political radicalisation into violent action" (p. 261). In sum, in order to explain terrorist acts, SAT suggests that we need in the first place to understand how individuals come to believe in and perceive terrorism as a legitimate avenue of action. According to this theoretical framework, this cognitive perception–choice process results from the lasting exposure to radicalizing settings in which people come to be gradually exposed to cognitive frames and moral teachings

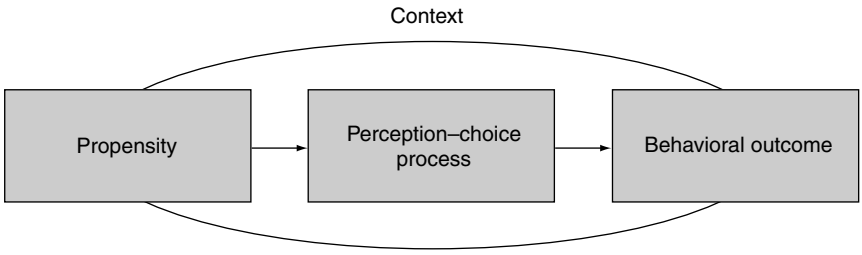


Figure 6.1 Situational action theory: simplified framework.

that validate involvement in clandestine political violence as a legitimate action avenue for them. Therefore, it appears crucial for scholars to explore how such cognitive schemes come to get incorporated by individuals and how they are shaped by broader social environments and activity fields in which they are embedded, as well as how these various social settings might evolve over time towards more radicalizing settings. Overall, the SAT forces us to pay closer attention to the interactionist and relational dynamics that sustain an individual's cognitive conversion toward a "terrorist mind" (Horgan, 2007, p. 21) or "extreme thinking" (Bronner, 2009).

The decision on whether or not to become involved in acts of terrorism comes at the end of the cumulative result of cognitive transformations shaping an individual's worldview. It is precisely this subjective evolution of meaning perspectives, beliefs and guidance rules, what Crenshaw (2011) describes as "subjective realities" (p. 88), that it is important to capture in order to reconstruct each stage of a "terrorist career." This task cannot be accomplished without a closer look at the relational settings—in other words, the radical sociability—in which people are embedded in their everyday life. Beliefs, intentions and goal formation are all mental processes that develop at the intersection of individual stories and social interactions that happen in various spheres of our life. Using the SAT in this context requires an understanding of how these processes of perception–choice are made possible in the first place through radicalizing settings that individuals become part of. To capture these key processes leading to the change of certain individual beliefs and guidance rules, we must first interrogate the emergence of radicalizing influences and the role that these relational settings, in turn, play in an individual's development of a terrorist propensity. Finally, how individuals come to be gradually inserted into radicalizing settings and social networks remains the key question that must be answered to explain radicalization processes.

The making of radical sociability: a multidimensional approach to radicalization

Before people can be exposed to a radicalizing influence, radicalizing settings have to be present in their direct social environment. Following the SAT framework, the radicalization process results in individuals' lasting exposure to radicalizing settings and influences in the social world. Thus we must explore how in the first place people come to be inserted within these particular kinds of socializing settings, if we truly intend to understand how individuals acquire their propensity, and in some cases endorse their intentionality, to engage in terrorism-related activities.

Online and offline life-spheres as field(s) of socialization: structure of meaning and sociability

Our daily life is composed of a plurality of socializing settings experienced through our life-spheres, which constantly help to define our worldviews, and

inform the rationality behind our actions. Life-spheres can be defined as "distinct though interrelated 'regions' in the life of an individual, each one with its own borders, logic, and dynamic" (Passy and Giugni, 2000, p. 121). This concept of life-spheres designates symbolic environments and fields of socialization (family, friendships, etc.) through which individuals experience particular socializing settings that contribute in turn to shaping their beliefs and social identity. For Passy and Giugni (2000):

> Life-spheres are interconnected. In other words, although they have well-defined borders and specific codes, life-spheres are constantly interacting. It is precisely this interaction that shapes the actors' structure of meaning.
>
> (Passy and Giugni, 2000, p. 122)

In sum, the—homogeneous or heterogenous—configuration of life-spheres constrains the frontiers of the cognitive market that individuals are able to access, and affect the overall rationality guiding people's actions. At the individual level, life-spheres operate as cognitive filters to ideas and beliefs circulating in the social world. Life-spheres, which can be online and/or offline, have a key role in the selective exposure to new socializing settings and the acquisition of new beliefs, motivations and guidance rules by individuals. As noted by Bronner (2009): "On average, beliefs that we endorse are probabilistically linked to the characteristics of cognitive market in which we are embedded voluntarily or involuntarily"[10] (p. 206). Accordingly, it is conceivable that the endorsment of extremist beliefs by a person, and therefore that person's propensity to see terrorism as a legitimate avenue of action, operates according to the same logic of selection and mechanisms of exposure.

Not all life-spheres are equally important in a person's life. Their importance is relative to the frequency of their activation. The more frequently life-spheres are activated, the more likely they will become important in a person's life, and in return facilitate that person's exposure to certain socializing settings. On the contrary, the less frequently a life-sphere is activated by a person, the more likely it will tend to occupy a marginal position in comparison to other life-spheres. The hierarchy of life-spheres in people's lives is therefore neither fixed nor permanent, but rather subject to various changes and evolutions over time. Sociability refers to the configuration where a stable hierarchy of life-spheres exists, in time and space, within a person's life (see Figure 6.2). Sociability produces a situational configuration from which an individual will derive his beliefs and his perceptions about the external world.

In other words, sociability should be understood as a stable configuration of individuals' socializing settings, which constrain people in their exposure to external social influences. Changes in beliefs and social identity are therefore highly correlated to the transformation of an individual's sociability, that is to say the re-ordering of the hierarchy of life-spheres in a person's life. What is to be explored in radicalization processes is the emergence of a radical sociability, in other words the re-ordering of the hierarchy of life-spheres opening

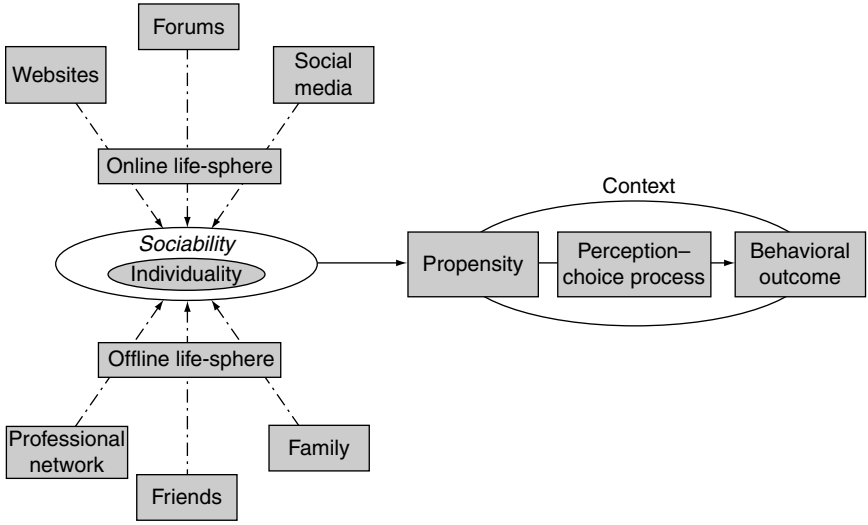


Figure 6.2 Online and offline life-spheres and the production of a sociability.

unprecedented avenues for an individual's lasting exposure to radicalizing settings. The emergence of radical sociability can take several forms, but it mainly consists of a shifting process by which new online and/or offline life-spheres and new socializing settings promoting a radical worldview come to be incorporated in the original life-sphere hierarchy of a person's life.

The emergence of a radical sociability: interlocking patterns

According to this theoretical framework, the Internet should be considered in itself as a life-sphere among others and therefore a symbolic environment and field of socialization, which can facilitate an individual's exposure to particular socializing settings. If family, friends and professional entourage represent various examples of offline life-spheres that participate in shaping individual sociability, virtual milieus—websites, discussion forums and social media platforms—can be considered as common examples of online life-spheres. Online and offline life-spheres each have their own characteristics and tend to produce different socializing settings, which can be largely independent from each other or deeply interrelated depending on a person's life-sphere configuration. In many cases, online and offline life-spheres do not necessarily overlap, leaving opportunities for a person's life-sphere hierarchy to change and be reevaluated. With the issue of radicalization processes in mind, the fact that these life-spheres do not necessarily intertwine is very important as this diminishes the risk of an enduring homogeneous exposure to radicalizing settings. The fact that all life-spheres of an individual do not fully intertwine together deeply contributes to

creating a moderating effect on radicalizing settings which an individual might be exposed to. On the contrary, when an individual's online and offline life-spheres tend to become highly interlocked, linkages that people have established between their various life-spheres tend to reinforce particular socializing settings and a particular type of sociability. Accordingly, the emergence of a radical sociability can result from radicalizing settings being turned into a crucial and central element in all an individual's life-spheres, thus confining him/her to a gradual cognitive monopoly that will lead to the progressive crystallization of his/her beliefs and social identity, both online and offline. In the example in Figure 6.3, friends, forums and social media all represent life-spheres with radicalizing settings that tend to gradually occupy a more and more important space in a person's life, contributing in turn to the interlocking pattern that will allow the emergence of a radical sociability.

Conclusion

To summarize my theoretical argument, the more an individual's life-spheres become intimately interlocked in a person's life, the more this configuration will lead that person to be exposed to similar socializing settings. In the case of terrorism and clandestine political violence, one life-sphere alone cannot produce the emergence of a radical sociability; rather, it is the convergence of all of an individual's life-spheres in which radicalizing settings are present that will tend to produce such a homogeneous exposure. It is possible that the emergence of a radical sociability may create a constant process of self-interactions that allows individuals to reinforce their beliefs and social identity as well as their embeddedness in specific

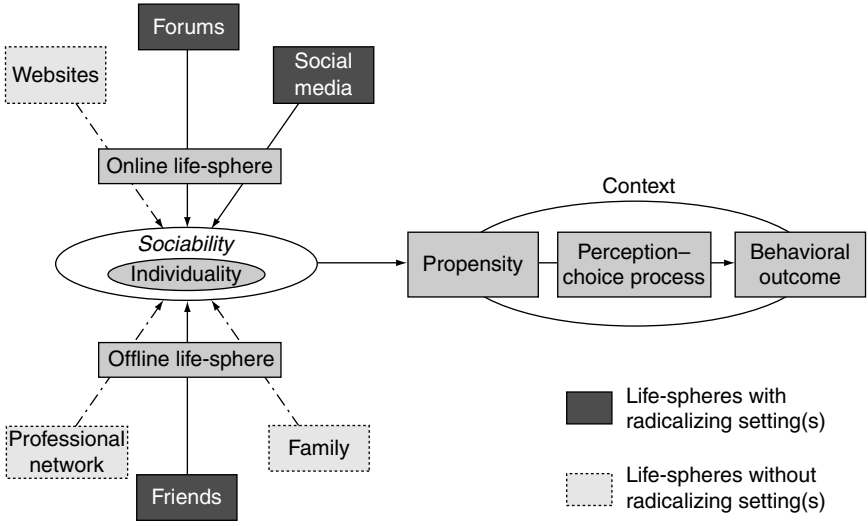


Figure 6.3 The emergence of a radical sociability.

social networks and milieus. In the light of this theoretical approach to radicalization, it is possible to suggest that the role of the Internet in radicalization phenomena cannot be understood without a closer examination of the relational setting through which some individuals come to acquire a propensity to perceive involvement in terrorism-related activities as a legitimate action alternative. The Internet alone does not radicalize people; rather, it represents one life-sphere among others, one piece of the puzzle among many.

What ought to be explained in radicalization phenomena related to digital networks is how the Internet interacts with other life-spheres and how it makes possible the emergence of a particular kind of sociability: the radical sociability. Only by recasting our approach to radicalization in such a theoretical perspective will we be able to assess what is exactly the circumstantial role of the Internet in the making of terrorist trajectories and pathways towards clandestine political violence.

Notes

1 I use here the concept of "terrorism" according to Charles Tilly's definition understood as an "asymmetrical deployment of threats and violence against enemies using means that fall outside the forms of political struggle routinely operating within some current regime" (Tilly, 2004, p. 5). Although other authors use terms such as "clandestine political violence" (Della Porta, 2013), I prefer here to use the term "terrorism" because it covers a large spectrum of extraordinary violent actions by individuals or clandestine groups for political purposes.

2 For the purpose of this chapter, I use a broad definition of "Internet" that interchangeably encompasses terms such as "the Internet," "the web," "digital networks" or "cyberspace."

3 The term "career" is mobilized in this chapter in its sociological acceptation. This concept of "career" has been developed and repeatedly used to understand the process by which people come to get engaged in various activities such as "deviant and criminal careers" (Becker, 1963; Matza, 1969). Applied to clandestine political violence and terrorism, the notion of "career" allows us to understand how, at each biographical stage, the attitudes and behaviors of individuals engaged in terrorism involvement trajectories are constructed by the permanent dialectical process between their own individual history and the socializing settings to which they are exposed. A career approach consequently involves a theoretical perspective that needs to take in consideration both the "subjective shift" of individuals' belief systems about the external world and the "objective transformation" of social settings in which individuals come to be embedded.

4 Personal interviews with anti-terrorist police officials and judges in the United Kingdom, Belgium, France and Canada.

5 For an extensive bibliography of the multi-faceted relationships between terrorism and the media, including the Internet, see Tinnes, 2013.

6 As I consider cyberterrorism a different phenomenon, this chapter does not attempt to cover the literature on this topic. Cyberterrorism is defined here as "highly damaging computer-based attacks or threats of attack by non-state actors against information systems when conducted to intimidate or coerce governments or societies in pursuit of goals that are political or social" (Denning, 2007).

7 In accordance with framing theory, I define frames as schemata of interpretation that allow people to make sense of the social world. Frames help people to render their

own social reality meaningful and therefore "to organize experience and guide action, whether individual or collective" (Snow, Rochford, Worden and Benford, 1986, p. 464).

8 See for exemple Von Behr, Reding, Edwards and Gribbon (2013).

9 For an extensive discussion of the case for applying situational action theory to the study of terrorism and political violence, see Bouhana and Wikström (2010 and 2011).

10 Translation by the author.

References

Amble, J. C. (2012) Combating terrorism in the new media environment. *Studies in Conflict and Terrorism.* 35 (5), pp. 339–353.

Archetti, C. (2012) *Understanding Terrorism in the Age of Global Media: A Communication Approach.* New York: Palgrave Macmillan.

Awan, A. A. (2007) Virtual jihadist media: Function, legitimacy and radicalizing efficacy. *European Journal of Cultural Studies.* 10 (389), pp. 389–408.

Back, L., Keith, M. and Solomos, J. (1998) Racism on the Internet: Mapping neo-fascist subcultures in cyberspace. In Kaplan, J. and Bjørgo, T. (eds) *Nation and Race: The Developing Euro-American Racist Subculture.* Boston: Northeastern University Press.

Bartlett, J., Birdwell, J. and King, M. (2010) *The Edge of Violence: A Radical Approach to Extremism*. London: Demos.

Becker, H. S. (1963) *Outsiders: Studies in the Sociology of Deviance.* New York: Free Press of Glencoe.

Benson, D. (2014) Why the Internet is not increasing terrorism. *Security Studies*. 23 (2), pp. 293–328.

Bermingham, A., Conway, M., McInerney, L., O'Hare, N. and Smeaton, A. F. (2009) Combining social network analysis and sentiment analysis to explore the potential for online radicalization. *Social Network Analysis and Mining*. ASONAM'09 International Conference on Advances, pp. 231–236.

Bjelopera, J. P. (2011) *American Jihadist Terrorism: Combating a Complex Threat.* Washington DC: Congressional Research Service.

Bolt, N. (2012) *The Violent Image: Insurgent Propaganda and the New Revolutionaries.* New York: Columbia University Press.

Bormann, E. G. (1972) Fantasy and rhetorical vision: The rhetorical criticism of social reality. *Quarterly Journal of Speech.* 58 (4), pp. 396–407.

Borum, R. (2011a) Radicalization into violent extremism I: A review of social science theories. *Journal of Strategic Security.* 4 (4), pp. 7–36.

Borum, R. (2011b) Radicalization into violent extremism II: A review of conceptual models and empirical research. *Journal of Strategic Security.* 4 (4), pp. 37–62.

Bouhana, N. and Wikström, P.-O. H. (2010) Theorizing terrorism: Terrorism as moral action. *Contemporary Readings in Law and Social Justice*. 2 (2), pp. 9–79.

Bouhana, N. and Wikström, P.-O. H. (2011) *Al Qa'ida-Influenced Radicalisation: A Rapid Evidence Assessment Guided by Situational Action Theory*. Home Office Occasional Paper 97. London: Research, Development and Statistics, Office for Security and Counter-terrorism, Home Office.

Bowman-Grieve, L. (2009) Exploring "Stormfront": A virtual community of the radical right. *Studies in Conflict and Terrorism.* 32 (11), pp. 989–1007.

Bowman-Grieve, L. (2010) Irish republicanism and the Internet: Support for new wave dissidents. *Perspectives on Terrorism.* 4 (2), pp. 22–34.

Bowman-Grieve, L. and Conway, M. (2012) Exploring the form and function of dissident Irish Republican online discourses. *Media, War and Conflict.* 5 (1), pp. 71–85.

Brachman, J. M. (2009) *Global Jihadism: Theory and Practice.* New York: Routledge.

Briggs, R. and Strugnell, A. (2011) *Radicalisation: The Role of the Internet—A Working Paper of the PPN*. London: Institute for Strategic Dialogue.

Bronner, G. (2009) *La pensée extrême: Comment des hommes ordinaires deviennent des fanatiques.* Paris: Denoël.

Burris, V., Smith, E. and Strahm, A. (2000) White supremacist networks on the Internet. *Sociological Focus.* 33 (2), pp. 215–235.

Caiani, M. and Wagemann, C. (2009) Online networks of the Italian and German extreme right. *Information, Communication and Society.* 12 (1), pp. 66–109.

Caiani, M., Della Porta, D. and Wagemann, C. (2012) *Mobilizing on the Extreme Right: Germany, Italy, and the United States.* New York: Oxford University Press.

Campana, C. and Ducol, B. (2015) Voices of the "Caucasus Emirate": Mapping and analyzing North Caucasus insurgency websites. *Terrorism and Political Violence*. DOI: 10.1080/09546553.2013.848797.

Chen, H. (2008) Sentiment and affect analysis of dark web forums: Measuring radicalization on the internet. *Intelligence and Security Informatics*. IEEE International Conference, pp. 104–109.

Chen, H. (ed.) (2011) *Dark Web: Exploring and Data Mining the Dark Side of the Web*. London: Springer.

Chen, H., Chung, W., Qin, J., Reid, E., Sageman, M. and Weimann, G. (2008) Uncovering the dark web: A case study of jihad on the web. *Journal of the American Society for Information Science and Technology.* 59, pp. 1347–1359.

Ciovacco, C. J. (2009) The contours of Al Qaeda's media strategy. *Studies in Conflict and Terrorism.* 32 (10), pp. 853–875.

Cole, J. (2012) Radicalisation in virtual worlds: Second life through the eyes of an avatar. *Journal of Policing, Intelligence and Counter Terrorism.* 7 (1), pp. 66–79.

Conway, M. (2006) Terrorism and the Internet: New media—new threat? *Parliamentary Affairs.* 59 (2), pp. 1–30.

Conway, M. (2012) From al-Zarqawi to al-Awlaki: The emergence and development of an online radical milieu. *Counter Terrorism Exchange (CTX).* 2 (4), pp. 12–22.

Conway, M. and McInerney, L. (2008) Jihadi video and auto-radicalisation: Evidence from an exploratory YouTube study. Paper presented at EuroISI 2008—First European Conference on Intelligence and Security Informatics, Esbjerg, 3–5 December.

Coolsaet, R. (2011) Terrorism and radicalisation: What do we know? In Coolsaet, R. (ed.) *Jihadi Terrorism and the Radicalisation Challenge: European and American Experiences*. Burlington: Ashgate Publishing.

Crenshaw, M. (2011) *Explaining Terrorism: Causes, Processes and Consequences*. London: Routledge.

Dalgaard-Nielsen, A. (2010) Violent radicalization in Europe: What we know and what we do not know. *Studies in Conflict and Terrorism*. 33 (9), pp. 797–814.

De Koster, W. and Houtman, D. (2008) "Stormfront is like a second home to me." *Information, Communication and Society.* 11 (8), pp. 1155–1176.

Della Porta, D. (2013) *Clandestine Political Violence.* Cambridge: Cambridge University Press.

Denning, D. E. (2007) A View of Cyberterrorism 5 Years Later. In Himma, K. E. (ed.) *Internet Security: Hacking, Counterhacking, and Society.* Sudbury: Jones and Barlett Publishers.

Dolnik, A. (2013) *Conducting Terrorism Field Research: A Guide.* New York: Routledge.

Ducol, B. (2012) Uncovering the French-speaking jihadisphere: An exploratory analysis. *Media, War and Conflict.* 5 (1), pp. 51–70.

Duffy, M. E. (2003) Web of hate: A fantasy theme analysis of the rhetorical vision of hate groups online. *Journal of Communication Inquiry.* 27 (3), pp. 291–312.

Edwards, C. and Gribbon, L. (2013) Pathways to violent extremism in the digital era. *The RUSI Journal.* 158 (5), pp. 40–47.

Egerton, F. (2011) *Jihad in the West: The rise of militant Salafism.* New York: Cambridge University Press.

El Difraoui, A. (2013) *Al-Qaida par l'image: La Prophétie du martyre*. Paris: Presses Universitaires de France.

Fighel, J. (2007) Radical Islamic Internet propaganda: Concepts, idioms and visual motifs. In Ganor, B., Von Knop, K. and Duarte, C. A. M. (eds) *Hypermedia Seduction for Terrorist Recruiting.* Eilat: IOS Press.

Gartenstein-Ross, D. and Grossman, L. (2009) *Homegrown Terrorists in the U.S. and U.K.: An Empirical Examination of the Radicalization Process.* Washington DC: Foundation for Defense of Democracies.

Gerstenfeld, P. B., Grant, D. R. and Chiang, C.-P. (2003) Hate online: A content analysis of extremist Internet sites. *Analyses of Social Issues and Public Policy.* 3, pp. 29–44.

Gohel, S. M. (2009) The Internet and its role in terrorist recruitment and operational planning. *CTC Sentinel.* 2 (12), pp. 14–15.

Homeland Security Institute (2009) *The Internet as a Terrorist Tool for Recruitment and Radicalization of Youth.* Arlington: Homeland Security Institute.

Horgan, J. (2007) From profiles to pathways: The road to recruitment. *eJournal USA Foreign Policy Agenda.* 12 (5), pp. 24–25.

Hoskins, A. and O'Loughlin, B. (2009) Media and the myth of radicalization. *Media, War and Conflic*t. 2 (2), pp. 107–110.

Jacobson, M. (2010) Terrorist financing and the Internet. *Studies in Conflict and Terrorism.* 33 (4), pp. 353–363.

Janbek, D. and Prado, P. (2013) Rethinking the role of virtual communities in terrorist websites. *Counter Terrorism Exchange (CTX).* 2 (4), pp. 12–22.

Judy, M. (2011) Terrorism's virtual safe haven and the effects on terror operations. *Global Security Studies.* 2 (1), pp. 34–44.

Kenney, M. (2010) Beyond the Internet: Mētis, Techne, and the limitations of online artifacts for Islamist terrorists. *Terrorism and Political Violence.* 22 (2), pp. 177–197.

Kimmage, D. (2008) *The Al-Qaeda Media Nexus: The Virtual Network Behind the Global Message*. Washington DC: Radio Free Europe/Radio Liberty.

Kimmage, D. (2010) *Al-Qaeda Central and the Internet*. Washington DC: New America Foundation.

King, M. and Taylor, D. M. (2011) The radicalisation of homegrown jihadists: A review of theoretical models and social psychological evidence. *Terrorism and Political Violence.* 23 (4), pp. 602–622.

Klausen, J., Tschaen Barbieri, E., Reichlin-Melnick, A. and Zelin, A. Y. (2012) The YouTube jihadists: A social network analysis of Al-Muhajiroun's propaganda campaign. *Perspectives on Terrorism.* 6 (1), pp. 36–53.

Köhler, D. (2012) Internet and radicalization: Connecting the dots—The role of the Internet in individual radicalization process of right-wing extremists. Working Paper Series. Berlin: Institute for the Study of Radical Movements.

Kohlmann, E. F. (2008) Al-Qa'ida's MySpace: Terrorist recruitment on the Internet. *CTC Sentinel.* (1) 2, pp. 8–9.

Kohlmann, E. F. (2010) A beacon for extremists: The Ansar al-Mujahideen web forum. *CTC Sentinel.* (3) 2, pp. 1–4.

Lennings, C., Amon, K., Brummert, H. and Lennings, N. (2009) Grooming for terror: The Internet and young people. *Psychiatry, Psychology and Law.* 17 (3), pp. 1–14.

Lia, B. (2006) Al Qaeda online: Understanding jihadi Internet infrastructure. *Jane's Intelligence Review*. 2 December.

Lohlker, R. (ed.) (2013a) *Jihadism: Online Discourses and Representations.* Vienna: Vienna Universty Press.

Lohlker, R (ed.) (2013b) *New Approaches to the Analysis of Jihadism: Online and Offline.* Vienna: Vienna Universty Press.

Mandel, D. R. (2009) Radicalisation: What does it mean? In Pick, T. M., Speckhard, A. and Jacuch, B. (eds) *Home-Grown Terrorism: Understanding and Addressing the Root Causes of Radicalisation among Groups with an Immigrant Heritage in Europe.* Amsterdam: IOS Press.

Matza, D. (1969) *Becoming Deviant.* Englewood Cliffs: Prentice Hall.

McCauley, C. and Moskalenko, S. (2008) Mechanisms of political radicalization: Pathways towards terrorism. *Terrorism and Political Violence.* 20 (3), pp. 415–433.

Moghadam, F. M. (2005) The staircase of terrorism: A psychological exploration. *American Psychologist.* 60 (2), pp. 161–169.

Mozes, T. and Weimann, G. (2010) The e-marketing strategy of Hamas. *Studies in Conflict and Terrorism.* 33 (3), pp. 211–225.

Neumann, P. (2013) The trouble with radicalisation. *International Affairs.* 89 (4), pp. 873–893.

Neumann, P. and Kleinmann, S. (2013) How rigorous is radicalization research? *Democracy and Security.* 9 (4), pp. 360–382.

Neumann, P. and Stevens, T. (2009) *Countering Online Radicalisation: A Strategy for Action.* London: International Centre for the Study of Radicalisation and Political Violence (ICSR), King's College London.

Neuman, W. R. and Guggenheim, L. (2011) The evolution of media effects theory: A six-stage model of cumulative research. *Communication Theory.* 21 (2), pp. 169–196.

O'Callaghan, D., Greene, D., Conway, M., Carthy, J. and Cunningham, P. (2012) An analysis of interactions within and between extreme right communities in social media. Eprint arXiv:1206.7050. Available at: http://arxiv.org/pdf/1206.7050v1.pdf. Accessed 27 July 2014.

Pantucci, R. (2011) *A Typology of Lone Wolves: Preliminary Analysis of Lone Islamist Terrorists.* London: International Centre for the Study of Radicalisation and Political Violence (ICSR), King's College London.

Passy, F. and Giugni, M. (2000) Life-spheres, networks, and sustained participation in social movements: A phenomenological approach to political commitment. *Sociological Forum.* 15 (1), pp. 117–144.

Pisoiu, D. (2013) Coming to believe "truths" about Islamist radicalization in Europe. *Terrorism and Political Violence.* 25 (2), pp. 246–263.

Precht, T. (2007) *Homegrown Terrorism and Islamist Radicalisation in Europe: From Conversion to Terrorism*. Copenhagen: Danish Ministry of Justice.

Ramsay, G. (2013) *Jihadi Culture on the World Wide Web.* New York: Bloomsbury Academic.

Ranstorp, M. (2007) The virtual sanctuary of Al-Qaeda and terrorism in an age of globalization. In Eriksson, J. and Giacomello, G. (eds) *International Relations and Security in the Digital Age*. London: Routledge.

RCMP (2009) *Radicalization—A Guide for the Perplexed.* Ottawa: Royal Canadian Mounted Police Publications.

Reid, E. and Chen, H. (2007) Internet-savvy U.S. and Middle Eastern extremist groups. *Mobilization: An International Quarterly.* 12 (2), pp. 177–192.

Reilly, P. (2011) *Framing the Troubles Online: Northern Irish Groups and Website Strategy.* Manchester: Manchester University Press.

Richards, R. (2011) The problem with "radicalization": The remit of "prevent" and the need to refocus on terrorism in the UK. *International Affairs.* 87 (1), pp. 143–152.

Rogan, H. (2006) *Jihadism Online: A Study of how Al-Qaida and Radical Islamist Groups use the Internet for Terrorist Purposes.* Kjeller: Norwegian Defence Research Establishment.

Rogan, H. (2007) Abu Reuter and the e-jihad: Virtual battlefronts from Iraq to the Horn of Africa. *Georgetown Journal of International Affairs.* 8 (2), pp. 89–96.

Roversi, A. (2008) *Hate on the Net: Extremist Sites, Neo-Fascism On-line, Electronic Jihad.* Burlington: Ashgate.

Sageman, M. (2004) *Understanding Terror Networks.* Philadelphia: University of Pennsylvania Press.

Sageman, M. (2008) *Leaderless Jihad: Terror Networks in the Twenty-First Century.* Philadelphia: University of Pennsylvania Press.

Schmid, A. P. (2013) Radicalisation, de-radicalisation, counter-radicalisation: A conceptual discussion and literature review. ICCT Research Paper. The Hague: International Center for Counter-terrorism.

Schuurman, B. and Eijkman, Q. (2013) Moving terrorism research forward: The crucial role of primary sources. ICCT Background Note. The Hague: International Center for Counter-terrorism.

Sedgwick, M. (2010) The concept of radicalization as a source of confusion. *Terrorism and Political Violence.* 22 (4), pp. 479–494.

Seib, P. and Janbek, D. M. (2010) *Global Terrorism and New Media: The Post-Al Qaeda Generation*. New York: Routledge.

Silber, M. D. and Bhatt, A. (2007) *Radicalization in the West: The Homegrown Threat.* New York: New York Police Department.

Silke, A. (2010) The Internet and terrorist radicalisation: The psychological dimension. In Dienel, H.-L., Sharan, Y., Ahituv, N. and Rapp, C. (eds) *Terrorism and the Internet: Threats, Target Groups, Deradicalisation Strategies.* Amsterdam: IOS Press, pp. 27–40.

Sinai, J. (2012) Radicalisation into extremism and terrorism: A conceptual model. *The Intelligencer.* 19 (2), pp. 22–23.

Snow, D. A., Rochford, E. B., Worden, S. K. and Benford, R. D. (1986) Frame alignment processes, micromobilization, and movement participation. *American Sociological Review*. 51 (4), pp. 464–481.

Stenersen, A. (2008) The Internet: A virtual training camp? *Terrorism and Political Violence.* 20 (2), pp. 215–233.

Stenersen, A. (2013) Bomb-making for beginners: Inside an Al-Qaeda e-learning course. *Perspectives on Terrorism.* 7 (1), pp. 25–37.

Sutton, M. and Wright, C. (2009) Finding the far right online: An exploratory study of white supremacist websites. *Internet Journal of Criminology*, pp. 1–24.

Tateo, L. (2005) The Italian extreme right on-line network: An exploratory study using an integrated social network analysis and content analysis approach. *Journal of Computer-Mediated Communication*. 10 (2).

Taylor, M. and Horgan, J. (2006) A conceptual framework for addressing psychological process in the development of the terrorist. *Terrorism and Political Violence.* 18 (4), pp. 585–601.

TE-SAT (2013) *Europol TE-SAT 2013: EU Terrorism Situation and Trend Report*. The Hague: Europol.

Thomas, T. L. (2003) Al Qaeda and the Internet: The danger of "cyberplanning." *Parameters.* 23 (1), pp. 112–123.

Tilly, C. (2004) Terror, terrorism, terrorists. *Sociological Theory.* 22 (1), pp. 5–13.

Tinnes, J. (2013) Terrorism and the media (including the Internet): An extensive bibliography. *Perspectives on Terrorism.* 7 (1), pp. 145–147.

Torok, R. (2010) "Make a bomb in your mums kitchen": Cyber recruiting and socialisation of "white moors" and home grown jihadists. *Proceedings of the First Australian Counter-terrorism Conference*. Mount Lawley: Edith Cowan University.

Torres-Soriano, M. R. (2010) The road to media jihad: The propaganda actions of Al Qaeda in the Islamic Maghreb. *Terrorism and Political Violence.* 23 (1), pp. 72–88.

Torres-Soriano, M. R. (2012) Between the pen and the sword: The global Islamic media front in the West. *Terrorism and Political Violence.* 24 (5), pp. 769–786.

Torres-Soriano, M. R. (2013) The dynamics of the creation, evolution, and disappearance of terrorist Internet forums. *International Journal of Conflict and Violence.* 7 (1), pp. 164–178.

Torres-Soriano, M. R., Jordán, J. and Horsburgh, N. (2006) Analysis and evolution of the global jihadist movement propaganda. *Terrorism and Political Violence.* 18 (3), pp. 399–421.

Trévidic, M. (2013) *Terroristes: Les 7 piliers de la déraison*. Paris: JC Lattès.

Tsfati, Y. and Weimann, G. (2002) Www.terrorism.com: Terror on the Internet. *Studies in Conflict and Terrorism.* 25 (5), pp. 317–332.

Von Behr, I., Reding, A., Edwards, C. and Gribbon, L. (2013) *Radicalisation in the Digital Era: The Use of the Internet in 15 Cases of Terrorism and Extremism.* Cambridge/Brussels: RAND Europe.

Warner, B. R. (2010) Segmenting the electorate: The effects of exposure to political extremism online. *Communication Studies.* 61 (4), pp. 430–444.

Weimann, G. (2005) How modern terrorism uses the Internet. *The Journal of International Security Affairs.* (8).

Weimann, G. (2006a) *Terror on the Internet: The New Arena, the New Challenges*. Washington DC: United States Institute of Peace Press.

Weimann, G. (2006b) Virtual training camps: Terrorists' use of the Internet. In Forest, J. F. (ed.) *Teaching Terror: Strategic and Tactical Learning in the Terrorist World*. Lanham MD: Rowman and Littlefield.

Weimann, G. (2008a) Al-Qa'ida's extensive use of the Internet. *CTC Sentinel.* 1 (2), pp. 6–7.

Weimann, G. (2008b) Hezbollah dot com: Hezbollah's online campaign. In Caspi, D. and Samuel-Azran, T. (eds) *New Media and Innovative Technologies.* Beer-Sheva: Ben Gourion University Press.

Weimann, G. (2010) Terror on Facebook, Twitter and YouTube. *Brown Journal of World Affairs.* 16 (2), pp. 45–54.

Wikström, P.-O. H. (2004) Crime as alternative: Towards a cross-level situational action theory of crime causation. In McCord, J. (ed.) *Beyond Empiricism: Institutions and Intentions in the Study of Crime.* New Brunswick: Transaction Publications.

Wikström, P.-O. H. and Treiber, K. H. (2009) Violence as situational action. *International Journal of Conflict and Violence.* 3 (1), pp. 75–96.

Wikström, P.-O. H., Ceccato, V., Hardie, B. and Treiber, K. H. (2010) Activity fields and the dynamics of crime. *Journal of Quantitative Criminology*. 26 (1), pp. 55–87.

Wojcieszak, M. (2010) "Don't talk to me": Effects of ideologically homogeneous online groups and politically dissimilar offline ties on extremism. *New Media and Society.* 12 (4), pp. 637–655.

Zelin, A.Y. (2013) *The State of Global Jihad Online—A Qualitative, Quantitative, and Cross-Lingual Analysis*. Washington: New America Foundation.

7 Terrorist and extremist organizations' use of the Internet for recruitment

Garth Davies, Martin Bouchard, Edith Wu, Kila Joffres and Richard Frank[1]

Introduction

The recruitment of new members is vital for the continuity and stability of all organizations, including, and perhaps especially, terrorist groups and movements. In this respect, terrorist and extremist organizations are much like any other. At a minimum, sustaining the group's activities generally requires that they replace departing members. But new members or affiliates can also increase functional capacity in a number of ways. They may allow an organization to extend the scope of its enterprise by facilitating movement to new locations or by enabling larger, more complex or more labor-intensive operations. New recruits may also bring with them new connections, skills and ideas.

While recruitment is central to the viability of all groups, the process itself is not necessarily consistent across groups. That the means of recruitment are varied reflects, at least in part, the diversity of organizational milieus. The unique nature of terrorist and extremist organizations may present specific recruiting challenges and opportunities. One such opportunity is provided by the Internet, which by its very nature increases the visibility of extremist groups. Terrorist and extremist organizations can use the Internet to provide information about the group and its goals and to recruit individuals in various ways that do not involve active participation in actual violent incidents. Included in what we consider to be part of recruitment are group events and activities that can be promoted on the websites, calls for donations, or recruitment to a list of group members or sympathizers. Recruitment, seen in this way, includes raising awareness of the group and engaging broad support for its activities.

The objective of this chapter is to examine the extent to which extremist organizations use recruitment-related narratives and tools on their official websites, with a view to classifying websites in terms of the intensity of their recruitment efforts (from no efforts to passive, and finally to active recruitment efforts). To obtain the most complete picture possible, groups and organizations devoted to a variety of causes were sampled. It is important to note that the focus of the research presented here is on the more passive information diffusion element of Web 1.0, especially the information available on the public, official websites of these groups and organizations. These official websites are still relevant. They

are important in providing a "face" for the organization for anyone who wishes to get information on them, especially these Internet users who may not know a lot about the organization. They contain affiliation documents, videos, literature, donation forms, and information on past and upcoming events for members. This is not to deny the importance of Web 2.0 of Facebook and online discussion forums. The increased interactions afforded by these tools have doubtlessly aided the recruitment efforts of terrorist and extremists groups. Rather, the argument here is that Web 1.0 still has a role in the recruitment process and that the content of official websites remains severely under-researched.

Radicalization and recruitment online

The Internet has created an important distinction between recruitment into an organization and introduction to a more general social movement that may or may not lead to individuals taking action (other than spreading the word online). Individuals may develop and hold radical views, or participate in online forums, but never be recruited into any extremist or terrorist organization. Radicalization and recruitment are two distinct yet intimately related processes. Radicalization is essentially the precursor to recruitment. In general, radicalization is the process by which individuals come to adopt radical or extremist views and ideas (Taarnby, 2006). It is the process that prepares people to be receptive to recruitment. Recruitment, by way of contrast, involves practical steps taken to become an active member of an extremist group. It is the process of going operational (Jenkins, 2007). In the post 9/11 world, the Internet has become integral to both of these processes.

Recruitment has been identified by Conway (2006) as one of five core terrorist uses of the Internet. The very nature of the Internet, including ease of access and anonymity, affords extremist groups a number of advantages for recruiting. The international scope of the Internet enables groups to reach a much broader audience. This allows these groups to promote awareness of their cause and to convey their message to, and perhaps foster sympathy from, an international audience (Weimann, 2010). In short, the Internet creates a much larger pool of potential supporters and converts.

The Internet also increases opportunities for interactive communication (Conway, 2006), both between individuals and groups and among individuals. This dynamic draws people in and makes them feel as though they are contributing to the group and are part of a broader community. Instilling a feeling of belonging is a key element in the process of persuading individuals to support a movement. At the same time, the interactive capabilities of the Internet promote a more proactive approach on the part of extremist groups. Rather than wait for individuals to happen upon their websites, groups can attempt to persuade individuals with tailored messages.

New media technologies, including the Internet, have granted terrorists unprecedented freedom in crafting and delivering their messages and propaganda. Until very recently, traditional media sources functioned as gatekeepers, often

denying extremists a platform and drastically circumscribing their audience. The relationship between extremists and the mainstream media was once the subject of considerable debate. It used to be routinely typified as "symbiotic," but since 9/11 the relationship unequivocally has been altered and these groups have lost virtually all control over how they are portrayed in the mainstream media. The Internet has shifted the balance of control back to extremists: it is democratic (in terms of access), decentralized, and very difficult to restrict or censor in any meaningful or effective way (Tsfati and Weimann, 2002).

In conjunction with the changes in the recruiting landscape, the benefits of the Internet have proved to be too enticing for extremist groups to ignore. Indeed, that the Internet has become an integral part of extremist recruitment practices is no longer in doubt. The role of the Internet in relation to recruiting has raised a number of issues and questions, the most significant of which are addressed in the sections that follow.

Content

The increasing prominence of the Internet has, to some degree, blurred the lines between radicalization and recruitment. Several studies have noted that recruitment on jihadi websites is generally not overt. Instead, the strategy appears to be one of encouraging self-recruitment through radicalization. Brachman (2006) suggests that

> the jihadi movement is not simply using technological tools to recruit new members, receive donations, and plan attacks. In actuality, Al-Qaeda's use of the Internet and other new technologies has also enabled it to radicalize in order to precipitate violence and empower armies of new recruits by shaping their general worldview.
>
> (Brachman, 2006, p. 150)

Consistent with this strategy, Tsfati and Weimann (2002) found that information is the most common content on the jihadi websites they studied. In addition to standard fare about the history of the organization and biographies about important members, the websites also contain communiqués, publications, speeches and sermons. Together, these materials detail the groups' ideologies and political goals. These propaganda efforts are further supplemented by reference to the actions of those with whom the extremists are engaged. Directly attacking the enemy has been identified as the most common tactic used on these websites (Tsfati and Weimann, 2002). The overall presentation of information and "context" appears to operate on multiple levels. On one hand, there is a clear intention to prompt sympathy from the international community. But the rhetoric also appears calculated to provoke anger in a subset of the audience. In other words, the content displayed on these sites is not merely informational. Depending on how it is received, it can constitute the initial step on the road to radicalization, recruitment and violence.

Violence

Despite the fact that terrorist groups are dedicated to violence as a means of achieving their objectives, direct calls for violence on their websites are conspicuous by their absence. With few exceptions, such organizations avoid reference to the violent acts they have perpetrated. Violence may be encouraged obliquely, as in instances where the rhetoric includes "calls for jihad," or in the glorification of martyrs. Although "the legitimization and justification of violence can also be interpreted as an indirect call for violence" (Tsfati and Weimann, 2002, p. 327), these discussion generally are peripheral to the websites. Tsfati and Weimann (2002) speculate that the reluctance to showcase violence probably stems from the fact that image building is an integral facet of these groups' online presence.

Extremist groups may wish to downplay their own violence on the Internet, but they cannot refrain from discussing violence altogether. It is, after all, central to their endeavors. But rather than celebrate violence, groups dedicate considerable effort to justifying violence through a combination of four rhetorical devices (Tsfati and Weimann, 2002). First, extremist groups emphasize their weakness in relation to the state(s) that oppose them. Second, they have no choice but to resort to asymmetrical violence given the tremendous imbalance of power arrayed against them. Third, the use of force is relative. Terrorist groups point to the actions of authorities, characterizing them with charged terms such as slaughter, murder and genocide (Tsfati and Weimann, 2002). In essence, extremists argue that their violence pales in comparison to that of the state. Finally, these groups often contend that they would prefer to achieve their objectives through peaceful means, but the obstinance and belligerence of "the other side" prevents negotiated resolution and is therefore responsible for any bloodshed.

Targeting youth

In order for any organization to maintain its operations, it must continually attract new members. The vitality of social movements depends, at least in part, on their ability to entice young adherents, and the process of recruiting has always involved having some understanding of "where to look" for potential associates. Given the importance of online and virtual environments to the daily lives of teens and young adults, it is not surprising that extremists groups are turning to the Internet to target youths, even children. Today's youth lead hyperconnected lives. For many, the search for meaning, identity and community plays out on the Internet. Extremist websites are designed to draw in impressionable adolescents and address these identity issues.

The sophistication of the approach is evidenced by the age-graded nature of jihadi materials found on websites. For example, Hamas maintains a website, Al-Fateh, which is specifically designed for children (Weimann, 2006). Its presentation is in the style of a cartoon; it features colorful graphics and drawings,

songs, and children's stories. Mixed in with these elements, however, are pictures and messages glorifying suicide terrorists. Another vehicle for reaching children and youth is video games. Brachman (2006, p. 157) cites the example of a game, *The Resistance*, in which "players between the ages of five and seven become farmers in South Lebanon who join the Islamic resistance against invading Israelis. Their objective is to destroy all invading 'Zionist forces.' " Other video games are calibrated more for adolescents. Brachman notes that the quality of the graphics in these and other games is crude and "rudimentary." But the real danger is the underlying ideological message: Muslims everywhere are under attack, and the transgressors must be defeated for the sake of Islam. Video games catalyze awareness for the uninitiated, reinforce and deepen commitment in those already exposed to jihadi ideology, and offer new ways to induce youths into the resistance.

Web 2.0

The capacity of extremist groups to recruit on the Internet has been greatly enhanced by their embracing of Web 2.0 technologies. The original incarnation of the Internet, Web 1.0, is broad in its scope, but communication flows in only one direction. Web 2.0, in contrast, is premised on interactivity (Seib and Janbek, 2011). Technological advances have changed the nature of online communications for extremists, which now are focused much more on the social network aspects of the web. In addition to maintaining official websites, extremist groups have embraced the gamut of interactive tools, including chatrooms, instant messaging services, blogs, forums and social networking sites (Weimann, 2010). In fact, it has been suggested that Web 2.0 technologies have come to account for the bulk of extremists' online presence. Noguchi and Kholmann (2006) estimated that "90% of terrorist activity on the Internet takes place using social networking tools."

Web 2.0 is also a much more dynamic environment. Prior to 2003, most content on jihadi websites was text-based. Since that time, video content has played a much larger role (Conway and McInerney, 2008). While many of the early videos were accessible through Arabic-only websites, video sharing websites such as YouTube have expanded their reach exponentially. Importantly, YouTube also features file-sharing capabilities, which facilitates interaction between those who post materials and those who comment.

The advantages of Web 2.0 are clear. For those individuals surfing the net in hopes of connecting, of finding "community," the interactivity of sites such as Facebook, Twitter and YouTube is much more likely to act as a pull into the orbit of violent radicalism. It is the interactivity that promotes a sense of belonging, that make individuals feel that they are contributing to the cause, even if they are not operational. Research indicates that the virtual communities promoted by Web 2.0 "can be seen as important social arenas for the formation of interpersonal bonds, with the potential to contribute to individual involvement processes" (Bowman-Grieve, 2009, p. 1003).

Web 2.0 has not rendered extremist group websites obsolete. They continue to serve as easy points of entry for even the most casual web surfer. Websites also allow groups to maintain a modicum of control over the dissemination of information and materials. The advantages associated with Web 2.0 are not absolute. The democratization produced by interactivity has introduced a degree of chaos. Groups find their messages debated and challenged. The benefits of Web 2.0 are substantial, but there remains a place for group websites. There is perhaps no better evidence that the fact that extremist and terrorist organizations continue to build official websites, to update them and to expand their content. An official site serves as a place of convergence, a medium for advertisement which is especially salient to new or potential recruits who are not yet familiar with the message or the group.

Self-radicalization

The rise of self-radicalization, where small cells of "self-starters" coalesce around jihadi ideology but with few if any formal connections to larger groups such as Al-Qaeda, represents a profound paradigm shift in our understanding of the recruitment process. And the Internet has played a fundamental role in facilitating the emergence of these largely "do-it-yourself" groups. It has "effectively removed many of the practical barriers that once limited entry into the formal jihad" (Kirby, 2007, p. 425). Individuals that once would have had a difficult time moving beyond the status of Al-Qaeda sympathizer for lack of formal connections may now, on their own, graduate to being "full-fledged jihadists." Self-radicalization is a win-win proposition for extremist movements, which gain enhanced operational capacity (albeit undirected) while maintaining an arms-length distance that makes it that much more difficult for authorities to infiltrate their membership.

In addition to bringing together like-minded prospective extremists, the Internet contains a veritable treasure-trove of operational and tactical materials. "How-to" guides and videos, covering everything from making explosives to guerrilla warfare, may be obtained with relatively little effort. On various forums, manuals may be supplemented by trainers who are available to answer questions. Weimann (2006) has characterized the Internet as an "online terrorism university" for self-taught terrorists. The Internet has not yet become a full-blown "virtual training camp"; groups such Al-Qaeda do not appear to be organizing online training (Stenersen, 2008). But it is an invaluable resource library for the self-radicalized.

Homegrown extremists

High-profile cases such as the Toronto 18, the London Underground bombing and the Madrid train bombing have underscored the significance of homegrown extremism. Just as the Internet has abetted the advent of self-radicalized groups, so too is it implicated in the emergence of this threat. There is some disagreement about the precise definition of "homegrown." While it certainly encompasses those individuals who were born in the West, it has also been extended to those

who have studied in and/or immigrated to the West. The key consideration is citizenship. Individuals travelling from areas such as the Middle East, Northern Africa and selected parts of Asia have come under heightened scrutiny, making it more difficult for them to operate in Western countries (Michael, 2009). In contrast, individuals with passports from Western countries are less encumbered in their travels (Kirby, 2007). They arouse less suspicion and are more easily able to "blend in" and "fly below the radar."

While there is no definitive profile, and homegrown converts can come from any background (Horgan, 2003), diaspora communities (Awan, 2007) and Muslims who have had difficulty with cultural or social assimilation (Leiken, 2005) have garnered much of the attention. The precise role of the Internet in radicalizing these populations is uncertain. Most researchers concede that it plays a part, particularly during the initial phases of radicalization, but caution that face-to-face contact remains an important element in the recruitment of individuals from diaspora communities:

> The Internet is rarely the sole resource in jihadi recruitment; although the Internet serves a crucial purpose in exposing would-be jihadists to material and networks in the early stages of radicalization, it is often not the end of the road for the jihadist.
>
> (Mellen, 2012)

In relation to homegrown extremism, the Internet is but one of many potential "extremist incubators" (Silber and Bhatt, 2007).

Lone wolves

Although they have been relatively rare, incidents of "lone wolf" terrorism have captured the popular imagination. The image of the single terrorist, ostensibly acting alone, long predates the likes of Theodore Kaczynski, Timothy McVeigh, Eric Rudolph and Anders Breivik. But the Internet has, in Simon's (2013) words, "been a godsend for the individual terrorist" (p. 21). Drawing on Rapoport's (2004) conception of "waves" of terrorism, Simon argues that we are embarking on a new, "technological" age of terrorism. This new wave will not be dominated by any particular type of terrorism; rather, technology will be available for all to use. And the cornerstone of the technological wave is the Internet.

The Internet greatly amplifies the capacity of an individual to engage in extremist violence. But the most important aspect of the Internet may be its ability to keep lone wolves connected. Contrary to what the term implies, it appears that many lone wolves may not actually be alone. Weimann (2012) argues that while "they may operate alone, they are recruited, radicalized, taught, trained and directed by others" (pp. 78–79). The Internet allows those with lone wolf proclivities to balance isolation and connection. Individuals can be anonymous and "alone" while at the same time remaining connected to the world around them (Simon, 2013).

Background to the present study

It is important to consider online radicalization and recruitment in their proper context. There is at present little evidence to suggest that radicalization and recruitment can take place solely on the Internet. It is unlikely that the Internet will ever be able to completely replace human interaction, and social networks and relationships will continue to be paramount in the recruitment process. But the Internet does fulfill several important functions. First, it introduces the uninitiated to radical and violent ideologies and reinforces those ideologies for whom the ideologies were resonant. In other words, it helps to set the radicalization process in motion. Second, the interactive nature of the Internet allows for like-minded individuals to connect with each other, and with other social networks. The phenomena of self-radicalized groups and homegrown extremists are largely attributable to the architecture of the Internet. Finally, the Internet is a platform on which individuals spur each other toward recruitment as part of a radical game of one-upmanship.

> People egg each other on. They compare themselves to other activists. They realise that a lot more people are doing this than what it first seemed. Sometimes, there seems to be a competition for who can be the most radical.
>
> (Neumann and Rogers, 2007, p. 86)

Given that groups such as Al-Qaeda currently prefer "leaderless jihad" (Sageman, 2008), and that a focal point of their strategy is to encourage self-radicalization, homegrown extremism and lone wolves, there is every reason to believe that Internet support for recruitment will continue to grow in significance.

Prior analyses of extremist websites

Many writers have discussed the role of the Internet for terrorist groups, but few empirical studies have analyzed the content of websites. One exception is Seib and Janbek's (2011) overview of what is known on the content of terrorist groups' websites (especially Muslim groups), and the reasons for which these groups use the Internet. The researchers appropriately frame the Internet as a communication medium and proceed to summarize the process in terms of its message, its purpose and its audience. Their overview demonstrates that these groups use the Internet in much the same way and for the same reasons that non-terrorist groups do: to provide information on their organizations, their missions and their origins, and to try to generate awareness of the causes that motivate their existence. Because Seib and Janbek reviewed Muslim groups, the place of jihad in Islam is discussed on a majority of the websites they examined. Suicide attacks and martyrs who died or suffered for the cause are generally featured prominently on websites. Most sites contain pictures and videos depicting past military successes of the organization, members carrying weapons, and educational videos about the organization of jihad more generally. Some have

coverage of current events relevant to the organization, and most provide multiple ways to connect with the organization and its members via forums and comment forms. Seib and Janbek (2011; p. 48) summarize the online purpose and message of these organizations in this way: "these organizations are presenting themselves as religious and patriotic armed resistance movements and are accordingly sharing their missions and previous operations with their audience."

Seib and Janbek (2011) identify recruitment as one of the clear purposes of these websites. First, many of the organizations they reviewed offered an English version for their website, showing a concern for their image outside of their country of operation and an ambition to spread their message anywhere in the world. Second, although the target audience is definitely male, and the objective seems to incite them to join the movement, the authors found that an increasing number of websites contained material specifically targeting women or adolescents, suggesting a desire for expansion and recruitment within new audiences.

Further, Seib and Janbek (2011) provide a general list of elements to consider in analyzing the content of extremist groups' websites, and they establish a framework to make sense of these elements in the context of a communication process that includes "recruitment" as one of the key motives. But their analysis is presented in the form of a narrative review. As such, it lacks the systematic elements that could, for example, help classify the websites of the organizations reviewed as containing more or less violent content or as being more or less focused on recruitment.

Objective of the study

The objective of the present study is to examine the extent to which extremist organizations use recruitment-related narratives and tools on their official websites. In addition to being the first study to provide a classification of the types of recruitment patterns found in extremist organizations on the Internet, this study is also broader than previous research. The current literature on extremism and terrorism online has largely been focused on violent Islamic groups, notably those associated with the Al-Qaeda social movement. In light of this, the present study sought to analyze a variety of extremist groups falling outside of the violent jihad context (although overlaps do exist in some cases). We analyze extremist websites and organizations motivated by a variety of other causes. The websites of white supremacists are represented in our sample alongside those of extremist groups devotes to animal rights or the environment, as well as groups focused on localized conflicts and grievances.

Methods

Three elements of method and procedure helped us achieve our research objectives: (1) the selection of seed websites for analysis; (2) the creation of a recruitment scale and an extremism scale to classify the websites; and (3) the use of a web-crawler to extract information on the websites and map their egocentric networks.

Finding seed websites

The universe of seed websites used for the main analyses was primarily drawn from the Government of Canada's *Listed Terrorist Entities* (Public Safety Canada, 2014a). As stated in article 83.05 of the Criminal Code of Canada, the Anti-Terrorism Act provides measures for the Government of Canada to create a list of entities that:

- have knowingly carried out, attempted to carry out, participated in or facilitated a terrorist activity;
- knowingly acted on behalf of, at the direction of or in association with an entity that has knowingly carried out, attempted to carry out, participated in or facilitated a terrorist activity.

On their website, Public Safety Canada (PSC) specifies that the process begins with criminal and/or security intelligence reports on an entity disclosing the reasonable grounds to believe that it fits the above criteria. "If the Minister has reasonable grounds to believe that the above test is met, the Minister may make a recommendation to the Governor in Council to place the entity on the list" (Public Safety Canada, 2014b, para. 5).

It is important to note that no initial judgement call was made on whether the groups studied here should be qualified as "extremists" or not. Instead, the selection of groups to be sampled relied on the list of terrorist organizations found in the Canadian Criminal Code article 83.05. A starting point to constitute a sample was required, and this list is one of the few official documents publically available to use as sampling frame. It is in this spirit that the term "extremist organizations/groups" is used throughout this chapter. This study is interested in online content, not labels. The content of official websites was examined to evaluate the extent to which violent content was overtly displayed on the website, or the extent to which the narrative found on the website encouraged violent behavior. In the end, not all of the organizations studied displayed or encouraged any violence, but many of them did.

There are 53 organizations listed on PSC's website. A total of eight groups made it to the present study's final sample, including four that can be found on the list: Revolutionary Armed Forces of Colombia (FARC), Shaheed Kalsa (SK), Liberation Tigers of Tamil Eelam (LTTE) and Popular Front for the Liberation of Palestine (PFLP). These were the organizations for which an English-based information website existed and could be analyzed in the context of this study. To provide a broader range of extremist activities, this list was expanded to include organizations known to be active in Canada. Four other groups were added in this second step: Aryan Nations (AN), Loyal White Knights of the Ku Klux Klan (LWK), Earth First! (EF), and Animal Liberation Front (ALF). These eight entities were categorized into four types: religious, ideological (including both right-wing and left-wing), ethnic nationalist, and single-issue.

To generate a list of seed websites for the crawler, a Google search was performed using search terms that included the entity's name and related terms. The goal was to find the official website for the group or websites affiliated in some manner. If the name of the entity did not produce an official website, then the name of the entity with the search terms "official website" was entered into Google. If this still did not produce an official website, then known abbreviations of the entity were used (these were taken from informational websites on the organization that appeared during the initial searches). These abbreviations were then combined with the search term "official website" where no official website was found. During these searches, any extremist website (related or unrelated) was recorded. A list of one to 15 official or related websites was created for each entity. To produce the seed websites, this list was narrowed down to the official website (if found) or the most popular website (i.e., the website that featured earliest in the search). Often, the official and the most popular website were the same.

These websites were then analyzed in terms of their general characteristics (including an assessment of their level of extremism) and the extent to which they emphasize various elements of recruitment. Information collected on general characteristics of the websites included the website address, the date the website was visited, the type of website, and the number of pages and visitors. A summary of this information is provided in the Appendix to this chapter.

Constructing scales

The website extremism scale

There have been very few attempts to quantify the levels of extremism evident on terrorist websites (for one example of work in this area, see Stankov *et al*., 2010). The *extremism scale* utilized here is based on variations around two concepts. First, we examine whether the website actively encourages visitors to join the cause (or movement, or group). A website is considered to be "active" when it explicitly tries to elicit participation or to motivate visitors to action. "Passive" websites would merely provide information on the cause, without engaging directly with visitors on what they can do to support it.

Second, we examine whether the website contains content of a violent nature. Websites deemed to contain violent content would either have images/videos that clearly demonstrate acts of violence being perpetrated against or for the cause, or would contain text expressing violent ideas against another group (e.g., hate speech).

Merging these two concepts creates a four-point scale of extremism, as illustrated in Table 7.1. At the bottom of the scale (level 1) are websites that are informational only, and this information avoids clear presentation of violence or use of hate speech (such websites were designated "fact-based" websites). Level 2 websites would also avoid violence in the text or images presented, but they would actively encourage visitors to actively support the cause ("join-the-cause"

Table 7.1 The website extremism scale

	Violent	*Non-violent*
Active	Level 4 Call-to-violence	Level 2 Join-the-cause
Passive	Level 3 Displays-of-violence	Level 1 Fact-based

websites). Level 3 websites present material of a clearly violent nature without explicitly encouraging individuals into action ("displays-of-violence" websites). Finally, level 4 websites are those that actively encourage individuals into actions to support the cause, including violent actions ("call-to-violence" websites).

The website recruitment scale

In addition, each website was evaluated on a number of dimensions related to recruitment. These evaluations were then summarized via a *recruitment scale*, which attempts to capture the nature of the presence of recruiting on a website (Table 7.2). It is premised on the degree to which the website actively encourages action on the part of the viewer. The scale ranges from 0 to 3. At the lowest end, a score of 0 corresponds to "no recruiting presence." It indicates that the website displays no materials relevant to recruiting. The next level of recruitment presents what might best be considered the "first steps" toward recruitment. This "passive" recruitment suggests attempts to pique the curiosity of site visitors. It would include the presence of public forums or opportunities to subscribe to newsletters or magazines. A score of 2 on the recruitment scale connotes "indirection action." At this level, visitors are encouraged to support the cause and the actions of others. However, the website stops short of stimulating direct personal action. The clearest examples of "indirect action" are calls for donations. Finally, the highest range of the scale indicates "active" recruitment. It reflects encouragement toward direct action on the part of the potential recruit. This is the most varied of the recruitment categories; it includes things such as links to membership forms, announcements of (or invitations to) events, and overt calls to action.

Table 7.2 The website recruitment scale

Score	*Recruitment presence*
0	None
1	Passive
2	Indirect action
3	Active

The Terrorism and Extremism Network Extractor (TENE)

This study takes advantage of a web-crawler that automatically collects and analyzes online data. While some manual analysis is important, especially to understand the structure of websites and the content displayed in pictures and videos, sole reliance on manual analysis would have made many of our analyses impossible to do given the size of most of the websites under study (sometimes with thousands of pages to analyze). The web-crawler used in this study has been labeled the "Terrorism and Extremism Network Extractor" (TENE). TENE is a custom-written computer program that automatically browses the web for terrorism and extremism content. It was adapted from previous research studying child exploitation websites (Joffres *et al*., 2011). Westlake *et al*. (2011) provide a detailed discussion of how the web-crawler functions. For the purpose of this chapter, TENE was used to collect data on the frequency of recruitment-related keywords on the websites analyzed.

Results

Recruitment

The results of the recruitment analyses, summarized in Table 7.3, illustrate considerable variability across websites. On one end of the continuum, some websites dedicate significant resources to materials pertinent to recruiting. Recruitment is prominent, for example, on the Earth First! website, one of the few sites that includes a section explicitly focused on recruiting. EF offers a "Getting Involved" link to a website that encourages visitors to "Become an activist!," ("Join our treesitters and spend some time up in the crown of one of the huge redwood trees of California"), to "Become a volunteer" ("We always need extra people to hand out information and to organize events, such as fundraisers or demonstration, and for various other things") and to "Make a donation":

> Our treesitters need food, warm clothes and other goodies to safely stay in the trees over the winter, as well as tarps, plywood, and other miscellaneous building materials. We also welcome any kind of financial help you can offer, especially for our lawyer fees to fight the restraining order, which "Redwood Empire" tried to obtain against us.

The EF website also contains a wide assortment of media content and has a notable social media presence.

The Animal Liberation Front website similarly devotes considerable attention to recruitment. Although it does not have an explicit recruitment section, the ALF website features open access to materials, opportunities to make donations, and direct appeals for involvement. It includes several pages dedicated to activism in the form of a "To-Do" section. This section provides details on how to be engaged in activism, methods of activism (e.g., civil disobedience, demonstrations,

Table 7.3 The recruitment checklist

	AN	*LWK*	*FARC*	*LTTE*	*SK*	*PFLP*	*ALF*	*EF*
Explicit recruitment section	✓	✓	×	×	×	×	×	✓
Open access to materials	✓	×	×	✓	✓	✓	✓	✓
Direct appeal for involvement	✓	✓	×	×	✓	✓	✓	✓
Membership application	✓	✓	×	×	×	×	×	×
Membership fees charged	✓	✓	×	×	×	×	×	×
Requests/opportunities for donations/funding	✓	✓	×	×	×	×	✓	✓
Media content								
Videos	✓	✓	✓	✓	✓	✓	✓	✓
Games	×	×	×	×	×	×	✓	×
Photographs/images	✓	✓	✓	✓	✓	✓	✓	✓
Radio	✓	×	×	×	×	×	×	✓
Audio content (e.g., speeches)	✓	✓	✓	×	✓	×	✓	✓
Documents	✓	×	✓	✓	×	×	✓	✓
Artwork	✓	✓	×	×	×	×	✓	×
Other downloadable material	×	×	×	×	✓	×	✓	×
Social media								
Facebook	×	×	×	×	×	×	×	✓
Twitter	✓	×	✓	×	×	×	×	✓
YouTube	✓	✓	×	×	×	✓	✓	✓
Flickr	×	×	×	×	×	×	×	×
Guestbook	×	✓	×	×	×	×	✓	×
Other (please specify)	✓	×	✓	✓	×	×	×	✓
Subscriptions								
Magazine/e-zine	✓	×	✓	×	×	×	×	×
Newsletter	×	×	×	×	✓	✓	×	×
News aggregator/social news sites	✓	×	×	×	×	×	×	×
Forum	✓	✓	×	×	×	×	✓	×
Blog	×	×	×	×	×	×	×	✓
Merchandise	✓	✓	×	×	×	×	×	✓
Further contact information provided	✓	✓	×	×	✓	✓	✓	✓
Opportunities to volunteer	×	×	×	×	×	×	✓	✓
Directed toward more private sites	✓	✓	×	×	×	×	×	×
Events	✓	✓	×	×	×	✓	✓	✓
Recruitment scale	3	3	0	0	1	1	3	3

protests), where to be active (lists of events, demonstrations and volunteer options), and a handbook and guidelines on activism. The To-Do section encourages not only activism but also strategies of "education and communication" for "teaching your children and other beginners about animal rights" in ways that include "letter writing campaigns, [and] ideas for effective communication." As with EF, the ALF website contains substantial media content.

The websites for both the Aryan Nations and the Loyal White Knights of the Ku Klux Klan were also actively engaged in recruiting. The AN website is dominated by opportunities to participate and media highlighting these events.

Media content and the use of social media are more limited on the LWK website, but its tone nonetheless indicates that the main purpose of the website is recruitment. Attendance at events is critical for LWK supporters. Members must, for example, attend at least one rally per year to remain active, and the website is used to promote these activities.

While all four of these websites (EF, ALF, AN and LWK) are heavily oriented toward recruitment, there are several subtle but noteworthy differences in their approaches. First, only EF and ALF attempt to foster volunteerism. Offering opportunities for volunteers seems to reflect the more open and inclusive nature of these organizations. Conversely, the more exclusive character of groups such as AN and LWK is evident in how these groups approach membership. Both of these groups have a formal application process (with applications available on the webpages) and charge membership fees (which may be collected via the website). In a similar vein, AN and LWK also diverge from EF and ALF in that the former direct visitors to more private sites.

In contrast, the recruiting presence of the remainder of the websites was much less substantial. The Shaheed Khalsa (SK) and Popular Front for the Liberation of Palestine (PFLP) websites paid less attention to recruitment. SK's main recruitment method is a subscription to its Yahoo e-group, which appears prominently on the website's homepage and remains on the right-hand side of every webpage visited on the website. The option to subscribe to the e-group is repeated in a different format (without the logo) in a "Contact us" section of the website. Other opportunities to engage with the website include options to "contribute material" and separate email addresses for "general information" inquiries. While recruitment efforts within the website are mainly limited to the e-group subscription, this option follows the visitor everywhere on the website. The PFLP website demonstrates an analogous approach to recruiting. Outside of publicizing "events of solidarity" (i.e., lectures, speeches and brochure and poster distribution), there is little in terms of active or explicit recruitment; the majority of the website is designed to provide information on the PFLP, its cause and goals, and its members. There is, however, an option to subscribe to the PFLP newsletter which is ubiquitous, remaining on the right-hand side of every page visited within the domain.

At the lowest end of the spectrum, the websites for the Revolutionary Armed Forces of Colombia and the Liberation Tigers of Tamil Eelam are essentially unrelated to recruiting efforts. These sites exhibited limited media content and had minimal social media presences. Neither website provided means to directly engage with or support the organizations. Instead, these websites featured information and propaganda about the groups.

Keywords

To assist with gauging the intensity of recruitment efforts, TENE collected counts of specified keywords. The analysis presented in Table 7.4 indicates that certain recruitment-related words appear frequently across websites. By far the most recurring word is *member* (and its variant *membership*). For every group

Table 7.4 Keywords

	AN	*LWK*	*FARC*	*LTTE*	*SK*	*PFLP*	*ALF*	*EF*
Active	18.36	20.00	80.00	32.36	6.03	2.14	6.15	11.81
Application	0.05	480.00	0.00	20.30	2.66	0.79	0.40	5.79
Apply	0.09	13.33	0.00	0.00	1.42	0.70	0.83	3.62
Demonstration	0.06	0.00	0.00	4.29	1.42	2.37	2.06	1.74
Donate	0.01	26.67	0.00	0.00	0.35	0.00	25.75	142.35
Event	27.99	133.33	0.00	27.26	10.28	6.60	2.35	84.87
Join	97.28	253.33	160.00	6.66	74.11	7.44	6.33	54.95
Member	250.57	480.00	100.00	84.26	99.65	30.51	47.97	528.14
Membership	0.05	73.33	0.00	2.18	0.35	0.74	0.60	181.47
Merchandise	0.01	0.00	0.00	0.00	0.00	0.00	25.75	0.37
Newsletter	0.00	0.00	0.00	0.00	0.00	0.00	29.46	75.98
Protest	0.02	0.00	20.00	0.00	10.28	10.60	17.70	52.65
Recruit	0.02	6.67	40.00	0.02	1.77	0.70	0.94	0.69
Recruitment	0.01	0.00	0.00	7.67	0.89	0.19	0.11	0.33
Subscribe	97.18	0.00	0.00	0.00	1.95	0.00	0.36	47.15
Volunteer	0.02	0.00	0.00	0.00	56.91	0.56	2.39	158.37

except FARC, *member* is mentioned more often than any other keyword (and for FARC it places second). Another word common across all websites was *join*. The repeated use of these words clearly indicates the value that these groups place on association. Solicitations to be part of the organization comprised an important facet of their web-based strategies. Other keywords are found across websites, but at a much lower rate. Good examples would be the words *active* and *event*. All of the group encourage participation and almost all highlight particularly noteworthy activities, attendance at which allows viewers to increase their support for the cause.

There are also keywords that seem to be favored by particular groups. The word *subscribe*, for example, is found throughout the AN website, underlining the importance it places on its printed materials as a venue for connecting with potential recruits. There are several words, including *newsletter*, *protest* and *donate*, that have greater prominence on the ALF and EF websites. At the same time, some keywords that might reasonably be expected to be related to recruitment efforts were largely absent. Among the most conspicuous of these are the words *recruit* and *recruitment*. While signifiers of recruitment may be found across most websites, the word itself is avoided.

More generally, the results present in Table 7.4 suggest that, while there are some words that are routinely used in the context of recruiting, many of the group also pursue strategies that are unique to their circumstances.

Extremism

Figure 7.1 shows the levels of extremism (as well as recruitment) associated with each of the sample websites. None of the eight were characterized as

call-to-violence (Level 4) websites. That is, none of the websites combine the "violent" and "active" dimensions of the extremism scale (see Table 7.1). However, several websites feature *displays-of-violence* levels of extremism. These locations include violent images and/or rhetoric, but they remain "passive" to the extent that they do not overtly counsel violence. The SK website exhibits violence through posts that detail the murder, torture, imprisonment and massacres of Sikhs at the hands of the Indian government. There are also statements claiming that "it is necessary to launch a resolute campaign against the government's attacks, and be willing to pay any price in the process." But while violence is used to justify action in terms of seeking independence, the website does not go as far as overtly encouraging acts of violence. Visual violence, in the form of images of members carrying guns and employing guerrilla tactics, and a category dedicated to reporting conflicts, is also prominent on FARC's website. The AFL website displays violence through pictures of animals in deplorable living conditions or having been abused and articles on animal testing, hunting and killing. These images are then used to emphasize the need for action to rectify such abuses. As with SK, both websites stop short of explicitly promoting acts of violence in support of their causes.

With regard to extremism, the most common type of website is the *join-the-cause* variety. These websites are non-violent; their emphasis is on involvement. Perhaps the only element that unites that the AN, LWK, PFLP and EF websites is their shared belief in the "need to do something." Although these websites accentuate action, they differ by the degree to which they actually facilitate further participation. The EF website provides the greatest opportunities for direct engagement.

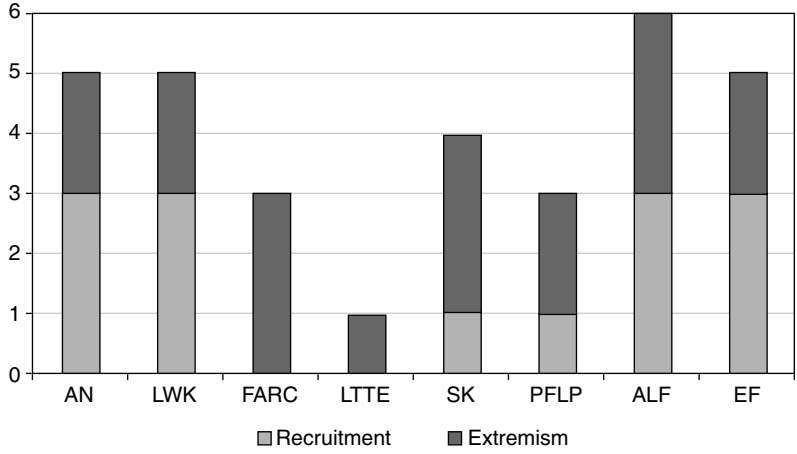


Figure 7.1 Recruitment and extremism scales (AN—Aryan Nations; LWK—Loyal White Knights of the Ku Klux Klan; FARC—Revolutionary Armed Forces of Colombia; LTTE—Liberation Tigers of Tamil Eelam; SK—Shaheed Kalsa; PFLP—Popular Front for the Liberation of Palestine; ALF—Animal Liberation Front; EF—Earth First).

It does not include membership materials, but this seems to be less a function of secrecy and security and related more to what might be termed a policy of "open recruitment." The AN and LWK make direct appeals for involvement, but their membership process is more guarded. The PFLP makes no allowances for membership; rather, it only provides "further contact information."

Finally, the LTTE is a prototypical example of a *fact-based* website. It contains minimal aggressive content. In fact, the website attempts to downplay or excuse violence perpetrated by the LTTE. Its sole focus is the presentation of information and context related to Tamils and the conflict in Sri Lanka.

Discussion

The results presented above clearly point to a wide range of approaches to Internet recruitment. The websites selected for analysis varied in terms of the extent to which they were explicitly oriented toward recruitment, as well as their respective levels of extremism. Taken together, however, several more general conclusions may be drawn from the case studies. These conclusions are discussed below.

Recruitment and extremism continuums

The websites analyzed in this study show clear differentiation along an "active–passive" continuum of recruitment efforts. The FARC and LTTE websites demonstrate virtually no recruitment presence, while SK and PFLP evince only passive attempts at recruitment. In stark contrast, the pages for both the right-wing groups (AN and LWK) and both the environmental/animal rights groups (ALF and EF) are heavily oriented toward recruitment.

Interestingly, the distinction between active and passive recruitment sites appears to be related to the group type. Groups that are grounded in more localized conflicts, be they in Colombia, Sri Lanka, Punjab or Israel–Palestine, are more passive in their recruitment efforts. Their primary focus seems to be on the presentation of information. Conversely, groups associated with more broad-based causes, here pertaining to racism or environment/animal rights, are much more overt in their attempts to promote direct participation and support.

There are similar, if not quite as pronounced, differences between websites with regard to their levels of extremism. At the lowest end of the scale, the emphasis of the LTTE website is the dissemination of information. There is considerable attention paid to violence, but the context is largely violence done to Tamils. As there is no explicit attempt to condone violence in response to persecution, this website scored low on extremism. In a like fashion, the PFLP webpage also devotes considerable attention to issues such as human rights and the persecution of Palestinians. Several other webpages, such as AN, LWK and EF, are also classified as predominantly non-violent. There is provocative rhetoric to be sure, but all stop well short of portrayals that could be unambiguously interpreted as condoning violence. Finally, three of the sites are classified as *passive-violent*. The most difficult

case is that of ALF. ALF is categorized along the violent continuum for its graphic depiction of animal suffering. It does not, however, promote violence in response. FARC and SK, on the other hand, both justify and rationalize violence as a necessary reaction to the provocations made against them.

It is noteworthy that there appears to be a moderate inverse association between levels of recruitment and extremism. The websites that are most actively engaging in recruitment eschew overt discussions of violence, while those with moderate to low recruitment presence are more likely to embrace violence. However, it is important to mention that the violence highlighted is always framed as "defensive." We will return to the theme of defensive violence below. The reason for the inverse relationship is unclear, but one might speculate that it could be related to the perceived breadth vs. depth of the potential pool of recruits.

A typology of recruitment websites

Based on the reconfigured (dichotomized) recruitment and extremism axes illustrated above, it is possible to identify a typology of recruitment websites. As demonstrated in Tables 7.5 and 7.6, the typology is comprised of four classifications, though only three were found for the purpose of this study. The first, *know us please*, refers to websites that are principally informational. As exemplified by the LTTE, these sites do not emphasize recruitment, but rather seek to make people aware of and explain their cause. Sites of this sort are also present with relatively low levels of extremism. Like the *know us please* websites, the second type of website, *support us because*, has a considerable informational component. In contrast to the *know us please* websites, however, *support us because* websites make more specific reference to violence, particularly justified defensive violence. Examples include the websites operated by FARC, SK and PFLP.

The final typology category that we found is *join us now*. These websites are strongly geared toward recruitment, but are less inclined to extremism than are the *support us because* sites. The websites that correspond with AN, LWK, ALF and EF are all examples of *join us now* websites. As our case studies did not reveal a single website that was high on both recruitment and extremism, there was no basis for including the final cell in Table 7.5 in the typology. Though we have not observed it, this category would, in all likelihood, be labeled as *act now with us* and would explicitly support violent action for the cause. Though not observed in this study, we include it in parenthesis as it is possible that future

Table 7.5 Typology of recruitment websites

		Extremism	
		Non-violent	*Violent*
Recruitment	*Passive*	Know us please	Support us because
	Active	Join us now	*Act now with us (not observed)*

Table 7.6 Typology of recruitment websites—examples

		Extremism	
		Non-violent	*Violent*
Recruitment	*Passive*	LTTE	FARC SK PFLP
	Active	AN LWK ALF EF	

studies might encounter such websites (or that such websites existed before and eventually disappeared when terrorism-related legislation on Internet content started to appear in most Western nations in the years following 9/11.)

Understanding the development of recruitment messages on the Internet

This study revealed an underlying process in the creation of website recruiting messages. The process appears to entail three more or less distinct phases. First, groups use their websites to develop a narrative. In every case, the narrative invokes some variant on the themes of oppression, injustice and abuse. The Sikh, Palestinian and Tamil populations are being oppressed by the Indian, Israeli and Sri Lankan authorities. Animals and the environment are subject to systematic abuse from a wide range of human activities. And right-wing groups see injustice in the changing nature of race relations. These narratives establish that the group has been wronged and is seeking legitimate redress for its grievances. They provide the foundation for the website.

Following the articulation of a coherent narrative, the second step in the process is the rationalization and justification of what we have referred to as "defensive" violence. In essence, these sites all claim that they must act to protect themselves, or those that are not capable of protecting themselves. Notice, however, that the contextualization of violence is very specific. None of the websites in the study openly condoned or encourage violence. This most likely reflects the fact that websites recognize the risk of being shut down if they "cross that line." Instead, these websites offer evidence of violence done against them and explain why they must respond.

For some groups, such as PFLP, LTTE and FARC, this is where the process of developing their recruitment message ends. Other groups, however, move to a third stage, offering opportunities for people to support or join the cause. The websites for these groups, including AN, ALF and EF, are the most clearly and extensively oriented toward recruitment. The results presented here suggest that the level of emphasis placed on recruitment by any website is not haphazard, but rather reflects strategic differences.

Appendix

Table 7.7 General characteristics of sampled websites

Group	*Aryan Nations (AN)*
Website address	www.aryan-nation.org
Date visited	25 September 2013 and 7 March 2014
Number of pages	101,927
Number of visitors	130,012
Group	*Loyal White Knights of the Ku Klux Klan (LWK)*
Website address	http://kkknights.com/
Date visited	28 September 2013 and 6 March 2014
Number of pages	15
Number of visitors	258,897
Group	*Revolutionary Armed Forces of Colombia (FARC)*
Website address	www.farc-ep.co/
Date visited	29 September 2013 and 7 March 2014
Number of pages	5
Number of visitors	Undisclosed
Group	*Liberation Tigers of Tamil Eelam (LTTE)*
Website address	www.eelam.com/ltte
Date visited	26 August 2013 and 9 March 2014
Number of pages	41,485
Number of visitors	Undisclosed
Group	*Shaheed Khalsa (SK)*
Website address	http://shaheed-khalsa.com/sukhdevbabbar.html
Date visited	24 August 2013
Number of pages	564
Number of visitors	Undisclosed
Group	*Popular Front for the Liberation of Palestine (PFLP)*
Website address	http://pflp – Popular Front for the Liberation of Palestine.ps/english/
Date visited	20 August 2013
Number of pages	2,150
Number of visitors	Undisclosed
Group	*Animal Liberation Front (ALF)*
Website address	www.animalliberationfront.com/
Date visited	24 August 2013
Number of pages	4,474
Number of visitors	17,984,265
Group	*Earth First (EF)*
Website address	www.earthfirst.org/
Date visited	20 August 2013
Number of pages	33,183
Number of visitors	491,508

Note

1 This chapter was prepared from a larger study on online recruitment funded by Public Safety Canada's Kanishka Program. The views expressed in this chapter, however, are solely those of the authors.

References

Awan, A. N. (2007) Virtual jihadist media. *European Journal of Cultural Studies.* 10 (3), pp. 389–408.

Bowman-Grieve, L. (2009) Stormfront: A virtual community of the radical right. *Studies in Conflict and Terrorism*. 32 (11), pp. 989–1007.

Brachman, J. M. (2006) High-tech terror: Al-Qaeda's use of new technology. *The Fletcher Forum of World Affairs.* 30 (2), pp. 149–164.

Conway, M. (2006) Terrorism and the Internet: New media, new threat? *Parliamentary Affairs.* 59 (2), pp. 283–298.

Conway, M. and McInerney, L. (2008) Jihadi video and auto-radicalisation: Evidence from an exploratory YouTube study. *Intelligence and Security Informatics*. 5376, pp. 108–118.

Horgan, J. (2003) The search for the terrorist personality. In Silke, A. (ed.) *Terrorists, Victims and Society: Psychological Perspectives on Terrorism and its Consequences*. Chichester: John Wiley and Sons, pp. 1–28.

Jenkins, B. (2007) *Building an Army of Believers: Jihadist Radicalization and Recruitment.* Testimony presented before the House Homeland Security Committee, Subcommittee on Intelligence, Information Sharing and Terrorism Risk Assessment. Santa Monica CA: RAND.

Joffres, K., Bouchard, M., Frank, R. and Westlake, B. (2011) Strategies to disrupt online child pornography networks. *Proceedings of the EISIC—European Intelligence and Security Informatics, Athens, September 2011*, pp. 163–170.

Kirby, A. (2007) The London bombers as "self-starters": A case study in indigenous radicalization and the emergence of autonomous cliques. *Studies in Conflict and Terrorism.* 30 (5), pp. 415–428.

Leiken, R. (2005) Europe's angry Muslims. *Foreign Affairs.* 84 (4), pp. 120–135.

Mellen, C. (2012) When Harry met Salifi: Literature review of homegrown jihadi terrorism. *Journal of Applied Security Research.* 7 (2), pp. 239–252.

Michael, G. (2009) Adam Gadahn and Al-Qaeda's Internet strategy. *Middle East Policy.* 16 (3), pp. 135–152.

Neumann, P. R. and Rogers, B. (eds) (2007) *Recruitment and Mobilisation for the Islamist Militant Movement in Europe*. London: Kings College, University of London.

Noguchi, Y. and Kholmann, E. (2006) Tracking terrorists online. *Washington Post*. 19 April. Available at: www.washingtonpost.com/wp-dyn/content/discussion/2006/04/11/DI2006041100626.html. Accessed 8 May 2014.

Public Safety Canada (2014a) *Currently Listed Entities*. Available at: www.publicsafety.gc.ca/cnt/ntnl-scrt/cntr-trrrsm/lstd-ntts/crrnt-lstd-ntts-eng.aspx. Accessed 15 June 2014.

Public Safety Canada (2014b) *About the Listing Process*. Available at: www.publicsafety.gc.ca/cnt/ntnl-scrt/cntr-trrrsm/lstd-ntts/bt-lstng-prcss-eng.aspx. Accessed 15 June 2014.

Rapoport, D. (2004) The four waves of terrorism. In Cronin, A. K. and Ludes, J. M. (eds) *Attacking Terrorism: Elements of a Grand Strategy*. Washington DC: Georgetown University Press, pp. 46–73.

Sageman, M. (ed.) (2008) *Leaderless Jihad: Terror Networks in the Twenty-First Century*. Philadelphia: University of Pennsylvania Press.

Seib, P. M. and Janbek, D. M. (eds) (2011) *Global Terrorism and the New Media: The Post-Al Qaeda Generation*. Abingdon: Routledge.

Silber, M. and Bhatt, A. (2007) *Radicalization in the West: The Homegrown Threat.* New York: New York Police Department.

Simon, J. D. (ed.) (2013) *Lone Wolf Terrorism: Understanding the Growing Threat*. New York: Prometheus Books.

Stankov, L., Higgins, D., Saucier, G. and Knezevic, G. (2010) Contemporary militant extremism: A linguistic approach to scale development. *Psychological Assessment*. 22, pp. 246–258.

Stenersen, A. (2008) The Internet: A virtual training camp? *Terrorism and Political Violence.* 20 (2), pp. 215–233.

Taarnby, M. (ed.) (2006) *Jihad in Denmark: An Overview and Analysis of Jihadi Activity in Denmark 1990–2006.* Copenhagen: Danish Institute for International Studies.

Tsfati, Y. and Weimann, G. (2002) Www.terrorism.com: Terror on the Internet. *Studies in Conflict and Terrorism*. 25 (5), pp. 317–332.

Weimann, G. (2006) *Terror on the Internet: The New Arena, The New Challenges.* Washington DC: United States Institute of Peace.

Weimann, G. (2010) Terror on Facebook, Twitter, and YouTube. *Brown Journal of World Affairs*. 16 (2), pp. 45–54.

Weimann, G. (2012) Lone wolves in cyberspace. *Journal of Terrorism Research*. 3 (2), pp. 75–90.

Westlake, B., Bouchard, M. and Frank, R. (2011) Finding the key players in child exploitation networks. *Policy and Internet.* 3 (2), pp. 1–32.

8 Exploring the behavioral and attitudinal correlates of civilian cyberattacks

Thomas J. Holt, Max Kilger, Lichun Chiang and Chu-Sing Yang

Research on terrorism and extremist activities has increased in the twenty-first century, most notably after the 9/11 terror attacks in the United States (Martin, 2006). These studies demonstrate the general prevalence of terror attacks globally (LaFree and Dugan, 2009; LaFree *et al*., 2009; Martin, 2006; Putnam, 2000), while a smaller proportion of studies have begun to identify correlates for involvement in terror, crime and violence generally (Chermak *et al*., 2013; Gruenewald *et al*., 2013; LaFree *et al*., 2009).

These studies greatly improve our understanding of terror activities, though there is generally little research on the use of technology in the facilitation of attacks against government infrastructure. Governments, defense agencies and financial institutions depend on technology in order to maintain databases of information and intellectual property and to communicate directly with the general public (Brenner, 2008; Jennings and Zeitner, 2003; Van Laer, 2010). Critical infrastructure, including telephony, water, sewer and power systems, are also managed via remote computer systems (Brodscky and Radvanovsky, 2011; Kilger, 2011).

As a consequence, computers and data are a key target for politically motivated attacks and social conflict (Brenner, 2008; Denning, 2011; Holt, 2009). Actors not sponsored by nation-states can leverage technological resources as a force multiplier to engage in non-violent actions such as protest, or serious forms of violence such as targeted attacks against infrastructure, with a greater magnitude than what might otherwise be possible through "real-world" protest or political action (Brenner, 2008; Jordan and Taylor, 2004; Kilger, 2011). The faceless, borderless nature of the Internet also allows individuals to efficiently mask their real identities and reduce the likelihood of their detection (Brenner, 2008; Denning, 2011). These conditions have given rise to "civilian cyberwarriors" who can operate without state sponsorship to attack various resources within their own governments or foreign nations due to the power differential provided by the Internet (Denning, 2011; Kilger, 2011).

Few researchers have considered what individual factors may predict participation in cyberattacks against either the home country or another nation. We define a cyberattack to include any attempt to cause economic, social or physical harm to a target via the use of hacking techniques (Denning, 2011; Kilger, 2011).

This exploratory study will examine these issues using an international sample of college students from a Midwestern US university and a major university in Taiwan. The findings provide initial insights about factors that predict individual willingness to take on the role of a cyberwarrior, including attitudinal, behavioral and technological factors. The implications of these findings for policymakers, intelligence communities and law enforcement are discussed in detail.

Exploring the relationship between political action on- and offline

Over the last 20 years, cyberspace has become an increasingly pertinent arena for the expression of political and ideological beliefs targeting governments and corporations alike (Al-Rizzo, 2008; Denning, 2011; Holt, 2009; Kilger, 2011; Woo *et al*., 2004). Many forms of cyberattacks can be situated in the larger spectrum of political expression commonly performed in the real world (Schmid, 1988, 2004). For instance, web defacements by politically motivated hacker groups are common following political events in the real world (Al-Rizzo, 2008; Denning, 2011; Kilger, 2011; Woo *et al*., 2004). In this sort of attack, an individual replaces the existing html code for a web page with an image and message that they have created. Defacements have become a regular tool for politically motivated hackers and actors to express their opinions (Denning, 2011; Holt, 2009; Woo *et al*., 2004).

There are similar forms of online action that can be used to engage in acts of vandalism and destruction, such as the infiltration of sensitive government networks in order to delete or otherwise destroy important information (Andress and Winterfeld, 2011; Denning, 2011). Access to such data might also lead an actor to reveal this knowledge to the general public to either embarrass or attack an institution, as with the release of diplomatic cables through Wikileaks (Sifry, 2011).

The unique technological aspects of cyberspace may present a barrier to individuals interested in engaging in violence against virtual targets. There is generally little research on the predictors of cyberactivism (Al-Rizzo, 2008; Holt, 2009; Stepanova, 2011; Vasi, 2006), though some of the correlates for cyberdeviance may also affect individual willingness to engage in cyberattacks. Those individuals who spend more time online may also be more likely to engage in certain forms of cyberattacks due to their familiarity with online spaces (Bossler and Burruss, 2011; Holt *et al*., 2010; Skinner and Fream, 1997). Technological skill may have little predictive capability, because individuals need not have significant knowledge of technology to engage in some forms of malicious online activity. Tutorials and tools are often freely available and used as a means to encourage unskilled actors to engage in attacks against various targets (Chu *et al*., 2010; Denning, 2011; Holt, 2009; Jordan and Taylor, 2004). Hacker groups and political attackers have distributed such resources over the last two decades in order to draw in interested parties to assist in attacks (Denning, 2011; Jordan and Taylor, 2004).

There may also be some tie between involvement in political actions in online environments and general participation in online deviance, particularly digital piracy. Those who engage in piracy tend to disregard copyright law and discredit the impact of their actions on private industry and governments (Higgins, 2005; Hinduja, 2001; Holt *et al*., 2010). Involvement in computer hacking may not, however, be associated with willingness to engage in cyberattacks. Over the last decade, the hacker group Anonymous have used simple point-and-click tools that can be downloaded by anyone, regardless of computer expertise, to engage in attacks against private industry and governments around the world (Correll, 2010; Poulsen, 2011). Thus involvement in cybercrime may have differential impacts on individual willingness to engage in cyberattacks.

An individual's attitudes toward various forms of cyberdeviance may also affect their willingness to engage in cyberattacks. The definitions and justifications that a person holds toward various forms of behavior can influence their willingness to engage in deviant behavior (Akers, 1998; Maruna and Copes, 2010; Sykes and Matza, 1957). Research suggests that individuals who favor the violation of computer laws and can justify their involvement in various forms of deviance are more likely to commit computer hacking and digital piracy (Holt *et al*., 2010; Ingram and Hinduja, 2008; Skinner and Fream, 1997). This relationship should have a similar impact on willingness to engage in cyberattacks against political targets, since they constitute a form of cybercrime.

Political attitudes held in the real world may be associated with online political activities, including cyberattacks (Holt and Kilger, 2012; Huddy and Khatib, 2007; Pettigrew, 2003; Schussman and Soule, 2005). Specifically, patriotism and nationalism are often significantly associated with political activity in the real world (Brewer, 1999; Kosterman and Feshbach, 1989; Schatz *et al*., 1999). Patriotism is often operationalized as the degree of pride one has in one's nation (Brewer, 1999; Kosterman and Feshbach, 1989); nationalism reflects the perception that a person's home country is better than others and should have global influence (Kosterman and Feshbach, 1989; Schatz and Staub, 1987). Those who report a high degree of nationalism and patriotism report more willingness to engage in attacks on foreign governments (Duckitt, 2003; Herrmann *et al*., 1999; Huddy and Khatib, 2007; Van Evera, 1994). Individuals with minimal nationalistic attitudes may be inclined to engage in political actions against their home country because they do not agree with its policies or stances (Terry *et al*., 1999; Conover *et al*., 2004). These variables may, however, have minimal relationships to online activities, as an individual can target any nation or group anywhere, including their home country (see Holt and Kilger, 2012; Van Laer, 2010).

An individual's perceptions of equality and minority groups may also increase willingness to engage in cyberattacks (Vollhardt, Migacheva, and Tropp, 2009). A strong belief in group equality may lead some to take action in support of a collective identity that is perceived as either ignored or marginalized (Friedkin, 2004; Lavis and Stoddart, 2003; Vollhardt *et al*., 2009). Attitudes toward marginalized groups in society may also serve as a disruptive force, since the

identification of an out-group can be used as a rallying point for social cohesion through targeted attacks against foreign entities (Kunovich and Hodson, 1999; Pettigrew, 2003; Post, 1998; Vollhardt *et al*., 2009). Individuals with minimal tolerance for out-groups in a society may also be less tolerant of different opinions and dissent from social norms (Kunovich and Hodson, 1999; Mummendey *et al*., 2001).

Finally, there are some demographic characteristics that may predict participation in different forms of political violence online. For instance, an individual's country of origin appears to differentially affect willingness to engage in political protest online. Citizens of democracies may be inclined to speak freely about their government on- or offline (Ayres, 1999; Earl and Schussman, 2003; Huddy and Khatib, 2007; Schatz *et al*., 1999), while individuals from repressive regimes may find less risk in protest actions in online environments where their identity can be shielded (Stepanova, 2011). In addition, males are more likely to engage in protest activities (Dalton, 2002; Verba *et al*., 1995), political violence (Putnam, 2000; Martin, 2006), and hacking and cybercrime generally (Bossler and Burruss, 2011; Hinduja, 2001; Skinner and Fream, 1997).

The present study

The potentially conflicting relationships between variables makes it difficult to identify the salient factors that may influence individual willingness to engage in politically motivated cyberattacks. Furthermore, these relationships may vary based on the target of an attack. This exploratory analysis will use an international sample of students to identify the correlates of three forms of cyberattack: individual willingness to engage in web defacements, searching government servers to engage in a WikiLeaks-style release of information, and compromising military servers to affect their readiness against both domestic and foreign targets.

Methods

Data for this study were generated from a self-report survey administered to undergraduate and graduate students at two universities: one in the United States and the other in Taiwan. These two nations were selected based on variations in their respective domestic and international relations and social policies. The US has long promoted and encouraged free speech and critical comments of government. Taiwan, however, only recently eliminated policies which sanctioned anti-government sentiment among the press and general public (CIA, 2013). Furthermore, the US has been a target for internal and external cyberattacks against government and industrial targets over the last two decades (Andress and Winterfeld, 2011). Though Taiwan does not appear to be a prominent target of cyberattacks, they have had difficult relations with China since the 1950s. The political challenges coupled with the Chinese military use of cyberwarfare (Andress and Winterfeld, 2011) give Taiwanese citizens a unique perspective

when compared to the US. Thus these groups provide purposive samples to identify different attitudes toward internal and external threats.

The US sample was collected at a large Midwestern university in the spring of 2010 using an online survey instrument. Using Dillman's (2007) Tailored Design Method, an email solicitation was delivered to a 25-percent stratified sample of the undergraduate and graduate student population. Respondents received a link to an electronic survey instrument along with the ethical guidelines of the study. A total of 357 individuals responded to the survey, which is a low response rate (5 percent of all recipients) but consistent with the overall trend of declining survey response rates (Curtin *et al*., 2005; Fan and Yan, 2010; Sheehan, 2001). The final sample size was 353 respondents due to missing data. The respondents were 60 percent male, which is slightly higher than the larger university composition (48 percent male). In addition, the proportion of domestic (89 percent) to international students (11 percent) reflects the general university composition as a whole.

Similar methods were used to develop the sample of Taiwanese students. A large research institution with comparable enrolments and student size was identified in order to generate a matched sample. Students from nine colleges were sent an email solicitation to the survey during the autumn of 2011, including 599 undergraduate and 305 graduate students. The response rate for this sample was 50 percent, which was substantially higher than the US, including 254 undergraduate and 202 graduate respondents ($n=444$). These response rates are not unusual given the distinct social dynamics present within Taiwanese university populations. This sample resembles the university's demographic composition (65 percent male; 92 percent international), and is comparable to the US sample. Thus, these samples provide a useful point of comparison to examine political action. The total combined sample size was 801 students, though 774 were included due to listwise deletion and missing data.

Critics commonly question the utility of college samples due to their limited generalizability (see Payne and Chappell, 2008). College students, however, provide a pertinent sample population to examine cyberattacks as they have various levels of computer skill, tend to be early adopters of technology, and participate in cyberdeviance (Higgins and Wilson, 2006; Hinduja, 2001; Holt *et al*., 2010; Skinner and Fream, 1997).Young people are also more likely to engage in protest activities in the real world (Wiltfang and McAdam, 1991) and online, as noted by their involvement in the hacker group Anonymous (Correll, 2010) and other forms of cyberprotest (Jordan and Taylor, 2004; Stepanova, 2011; Van Laer, 2010). Thus, college students are an appropriate population to study in order to explore the predictors for political action on- and offline.

Dependent variables

In order to examine willingness to engage in cyberattacks, respondents were presented with scenarios involving nation-state actions causing harm to the citizens of their home country. The study used a 2×2 factor design that involved the type

of attack and the identity of the nation-state causing the harm. A scenario design was employed due to the relatively limited proportion of individuals actively engaging in attacks against critical infrastructure on- and offline (Brenner, 2008; Martin, 2006). Scenarios have been used in a variety of criminological and political science research (Fishbein and Ajzen, 1975; Higgins, 2005; Nagin and Paternoster, 1993; Piquero and Bouffard, 2007) and appear to be valid constructs for actual behavior (Fishbein and Ajzen, 1975; Kim and Hunter, 1993). Thus, utilizing a scenario-based measure generates a reasonable data source to explore the phenomena of attacks against nation-states in cyberspace and the real world.

The first scenario presented to respondents required them to consider how they might react under the following conditions:

> Imagine that the country that you most closely associate as your home country or homeland has recently promoted national policies and taken physical actions that have had negative consequences to your country. These policies and actions have resulted in significant hardships for the people in your home country. What on-line activities do you think would be appropriate for you to take against your home country given their policies and physical actions? You may choose as many actions as you think the situation warrants. In this scenario, you may assume that you have the necessary skills to carry out any of the actions below.

Respondents were presented with a binary (yes/no) response for the following three items to perform in a cyber environment: (1) deface an important official government website for your home country[1]; (2) search your home country's government servers for secret papers that you might be able to use to embarrass the government; and (3) compromise one or more of your home country's military servers and make changes that might temporarily affect their military readiness.

The same language was used to assess individual willingness to engage in actions against a foreign nation-state inflicting harm on their homeland. This scenario utilized the fictitious nation of Bagaria as the source of harm to avoid prospective respondents' biases against either foreign nations or ethnic/racial groups.[2] The following language was used in the Bagarian scenario:

> Imagine that the country of Bagaria has recently promoted national policies and taken physical actions that have had negative consequences to the country that *you* most closely associate as your home country or homeland. These policies and actions have also resulted in significant hardships for the people in your home country.

The same response sets were presented to the respondent with the phrase Bagaria in place of "home country" to compare variations in action based on foreign or domestic targets. A limited proportion of respondents were willing to engage in these various attacks regardless of target. Nine percent were willing to engage

in web defacements, though between 10 and 13 percent were willing to search servers for data (see Table 8.1 for descriptive statistics). There was substantial variation in willingness to compromise military servers, with only four percent willing to target a server in their home country but nine percent willing to affect a Bagarian target.

Independent variables

Cybercrime variables

A range of independent variables were included in this analysis. Three measures were included to capture familiarity with and capacity for technological use, including the subjects' ability to: (1) use an operating system such as Unix or Linux; (2) use a standard computer programming or scripting language such as C++, Perl or Java; and (3) install an operating system such as Unix or Linux.[3] Response options ranged from "not at all comfortable" (1) to "very comfortable" (5) and provided a concise scale (alpha = 0.843) indicating the subjects' overall exposure to more technical computing skills.

Two scales were created to assess individual involvement in cybercrime. The first scale focused on digital piracy, as this is a common form of cybercrime

Table 8.1 Sample descriptives ($n = 774$)

Variables	*Mean*	*SD*	*Min*	*Max*
Deface government website, homeland	0.09	0.29	0	1
Deface government website, Bagaria	0.09	0.29	0	1
Search government servers, homeland	0.10	0.30	0	1
Search government servers, Bagaria	0.13	0.35	0	1
Compromise military servers, homeland	0.04	0.20	0	1
Compromise military servers, Bagaria	0.09	0.29	0	1
Time online	3.36	1.34	1	5
Computer skill	25.38	6.02	8	40
Piracy	4.73	2.62	2	10
Hacking	3.52	1.24	3	15
Ethics	2.74	0.90	1	4
People allowed	1.54	0.70	1	4
I should be able	2.33	0.98	1	4
Law enforcement quick	2.04	0.80	1	4
Hacking not a crime	1.84	0.77	1	4
Patriotism	18.63	3.61	6	24
Nationalism	6.41	2.30	3	12
Group equality	18.34	3.28	6	24
Outgroup antagonism	10.97	3.90	5	20
Physical actions, homeland	1.49	1.414	0	7
Physical actions, Bagaria	1.23	1.21	0	6
US	0.46	0.49	0	1
Gender	0.47	0.49	0	1

around the world (Holt *et al*., 2010; Ingram and Hinduja, 2008). Respondents were asked how often in the last 12 months they had knowingly used, made or given another person (1) a "pirated" copy of commercially-sold computer software; or (2) "pirated" media (music, television show or movie) (Holt *et al*., 2010; Skinner and Fream, 1997). Responses ranged from never (0), 1–2 times, 3–5 times, 6–9 times, and 10 or more times (4). These items were summed to assess frequency of participation in both forms of piracy (alpha = 0.759).

A second scale was created to capture respondents' involvement in computer hacking behaviors (Bossler and Burruss, 2011; Holt *et al*., 2010). Respondents were asked three questions regarding their involvement in the following behaviors over the last 12 months: (1) guessing another's password to get into his/her computer accounts or files; (2) accessing another's computer account or files without his/her knowledge or permission to look at information or files; and (3) adding, deleting, changing or printing any information in another's computer files without the owner's knowledge or permission (Bossler and Burruss, 2011; Skinner and Fream, 1997). Responses ranged from never (0), 1–2 times, 3–5 times, 6–9 times, and 10 or more times (4), and were summed to create a reliable scale in line with previous research (alpha = 0.725; Bossler and Burruss, 2011).

A series of attitudinal variables were included to understand the ways that perceptions about cybercrime may affect willingness to engage in cyberattacks. Respondents were presented with five items and asked to rate their agreement with that statement ranging from (1) strongly disagree to (4) strongly agree (Holt *et al*., 2010; Skinner and Fream, 1997). The first two measures assess agreement with definitions concerning the presence of online ethics: (1) *Rules:* there are clear rules on what is acceptable, ethical behavior online, and (2) *Use*: People should be allowed to use computers they don't own in any way they see fit.

Definitions favoring the violation of law were measured through the following items: (3) *Info:* I should be able to look at any computer information that the government, a school, a business or an individual has on me even if they do not give access. Perceptions of the presence of law enforcement were assessed through the following item: (4) *Law*: I believe that law enforcement groups are quick to recognize when a cybercrime occurs. Finally, the perception of cybercrime as acceptable was captured through (5) *Access*: Compared with other illegal acts people do, gaining unauthorized access to a computer system or someone's account is not very serious. Each item was included individually to identify what relationship it might have to willingness to engage in cyberattacks (see Bossler and Holt, 2010; Holt *et al*., 2010; Skinner and Fream, 1997).

Political variables

In order to assess the role that national identity or patriotism plays in individual decision-making, a factor score was created utilizing measures derived from Kosterman and Feshbach (1989). Respondents were asked to rate their agreement (1—strongly disagree; 4—strongly agree) with six items relating to their emotional connection to their home country: (1) I am proud to be a citizen of my

home country; (2) in a sense I am emotionally attached to my home country and am emotionally affected by its actions; (3) although at times I may not agree with the government, my commitment to my home country always remains strong; (4) I feel a great pride in the land that is my home country; (5) when I see my home country's flag flying I feel great; (6) the fact that I am a citizen of my home country is an important part of my identity. The responses to these six items were summed and provide a reliable scale (alpha = 0.850) measuring emotional attachment to their home country (see Table 8.1 for detail).

To consider the role of nationalism, a three-item scale was adapted from Kosterman and Feshbach (1989). These items assess the perception that the subject's home country is superior to other nations based on agreement with each sentiment (1—strongly disagree; 4—strongly agree): (1) other countries should try to make their government as much like my home country's government as possible; (2) generally, the more influence my home country has on other nations, the better off they are; (3) foreign nations have done some very fine things but my home country does things in the best way of all. The responses were summed to create a relatively parsimonious scale (alpha = 0.626) of respondents' support for nationalism.

Given the role of group equality as a predictor in protest activities (Vollhardt *et al*., 2009), a factor score was created using seven items adapted from Sidanius and Pratto (2001). These measures include: (1) it would be good if groups could be equal; (2) group equality should be our ideal; (3) all groups should be given an equal chance in life; (4) we should do what we can to equalize conditions for different groups; (5) we would have fewer problems if we treated people more equally; (6) we should strive to make incomes as equal as possible; and (7) no group should dominate in society. Respondents were asked to rate their agreement with these statements (1—strongly disagree; 4—strongly agree) and all responses were summed to create a reliable scale (alpha = 0.788). These items have been used to assess racism and prejudice (Sibley *et al*., 2006), and provide a practical metric to explore attitudes toward marginalized groups in society.

In order to assess out-group antagonism, five measures were adapted from Sidanius and Pratto (2001): (1) some groups of people are simply inferior to other groups; (2) if certain groups stayed in their place, we would have fewer problems; (3) it's probably a good thing that certain groups are at the top and other groups are at the bottom; (4) inferior groups should stay in their place; and (5) sometimes other groups must be kept in their place. Responses to each of these items (1—strongly disagree; 4—strongly agree) were summed (alpha = 0.833) to create a single scaled item.

An additive scale was created based on willingness to engage in various real-world protest activities in order to explore any relationship between political and social activism in on- and offline environments. In each scenario used to create the dependent variables of interest for this study, respondents were also asked to select what physical actions they would take in response to the perceived injustice from a set of eight items: (1) do nothing—let your country correct its actions on its own; (2) write a letter to your home country's government protesting their actions; (3) participate in a protest against your home country at an

anti-government rally; (4) protest at your home country's capitol building; (5) confront one of your home country's senior government officials about their policies; (6) sneak into a military base in your home country to write slogans on buildings and vehicles; (7) physically damage an electrical power substation in your home country; and (8) damage a government building in your home country with an explosive device. In the example for Bagaria, the phrase "your home country" was replaced with "Bagaria."

A scale was created by combining the binary measure for each of the seven physical action options together for both the homeland (alpha=0.596) and Bagarian (alpha=0.478.) scenarios. The "do nothing" item was excluded to assess active rather than passive forms of resistance. Though the reliability of these scales are generally low, alternative scales were generated using four and five items and included in the regression models presented below. While these items generally improved the reliability of the scale, they made no impact on the findings of the regression models (results not shown). All relationships remained consistent and at the same significance levels. Thus this seven-item scale is included here for the sake of replication of previous research in this area (Holt and Kilger, 2012). The scale corresponding to the home country or Bagarian targets is included in each set of regressions to identify the influence of willingness to engage in real-world cyberattacks across both domestic and foreign targets.

Demographic controls

Two demographic variables are included in these analyses based on the general literature on cybercrime and activism generally: respondent country and gender. A binary measure was included to capture whether the respondent was part of data captured in the US (1) or in Taiwan. Gender (0—male; 1—female) was included since hackers and individuals who engage in piracy tend to be male (Higgins, 2005; Holt *et al*., 2010; Skinner and Fream, 1997), and those who engage in physical protests and political violence generally tend to be male (Dalton, 2002; Martin, 2006; Verba *et al*., 1995).

Findings

Binary logistic regression models were created for each dependent variable (see Tables 2–4) based on homeland and Bagarian targets. Additionally, each regression had three models, one including the measures related to involvement in cybercrime, the second with political measures, and the third combining all variables together. Multicollinearity did not appear to bias the parameter estimates, as the independent variables were not strongly correlated with each other. Though the dependent variables are correlated with one another, the highest VIF and lowest tolerance were 3.122 and 0.320 respectively, suggesting that there are no issues with multicollinearity generally (results not shown).

Exploring the correlates for defacing government servers, regardless of target, suggests that there are few significant relationships present (see Table 8.2).

Table 8.2 Binary logistic regression models for defacing government servers ($n = 774$)

	Domestic			*Bagaria*		
	Model 1	*Model 2*	*Model 3*	*Model 4*	*Model 5*	*Model 6*
Variables						
Time online	0.182	–	0.111	0.160	–	0.104
	(0.103)		(0.115)	(0.102)		(0.116)
Computer skill	0.022	–	0.020	0.015	–	0.012
	(0.023)		(0.026)	(0.022)		(0.026)
Piracy	0.112*	–	0.100	0.052	–	0.034
	(0.052)		(0.058)	(0.052)		(0.059)
Hacking	0.105	–	0.078	0.073	–	0.080
	(0.086)		(0.094)	(0.088)		(0.093)
Ethics	−0.148	–	−0.134	−0.238	–	−0.416**
	(0.145)		(0.160)	(0.142)		(0.163)
People allowed	−0.069	–	−0.083	0.067	–	0.045
	(0.210)		(0.224)	(0.200)		(0.219)
I should be able	0.406**	–	0.361*	0.248	–	0.188
	(0.138)		(0.152)	(0.137)		(0.154)
Law enforcement quick	−0.077	–	0.066	−0.249	–	−0.167
	(0.172)		(0.193)	(0.174)		(0.196)
Hacking not a crime	0.069	–	0.088	0.240	–	0.346
	(0.169)		(0.184)	(0.166)		(0.187)
Patriotism	–	−0.071	−0.052	–	−0.046	−0.012
		(0.038)	(0.042)		(0.039)	(0.043)

Nationalism	–	0.003	0.011	–	−0.020	−0.015
		(0.066)	(0.076)		(0.069)	(0.084)
Group equality	–	0.013	0.022	–	−0.005	0.017
		(0.043)	(0.046)		(0.043)	(0.048)
Outgroup antagonism	–	0.145**	0.108	–	0.084*	0.032
		(0.044)	(0.062)		(0.041)	(0.064)
Physical actions, homeland	–	0.989***	0.987***	–	–	–
		(0.116)	(0.129)			
Physical actions, Bagaria	–	–	–	–	0.949***	0.982***
					(0.105)	(0.115)
US	0.610	–	−0.375	0.311	–	−0.606
	(0.339)		(0.554)	(0.328)		(0.543)
Gender	−0.465	–	−0.380	−0.805**	–	−751*
	(0.290)		(0.329)	(0.294)		(0.335)
Constant	−4.930***	−4.912***	−7.044***	−3.551*	−3.813**	−0.670*
	(9.61)	(1.376)	(1.826)	(0.929)	(1.313)	(1.842)
Model χ^2	45.464***	103.664***	126.319***	40.2758***	101.291***	131.259***
R^2	0.124	0.268	0.326	0.109	0.259	0.335

Notes
Unstandardized coefficients are presented with standard errors in parentheses due to space limitations; *$p<0.05$; **$p<0.01$, ***$p<0.001$. Pseudo R^2 are Nagelkerke R^2.

Interestingly, the political models have a better fit based on the Pseudo-R^2 statistic than the cybercrime measures in both models. In the domestic model with cybercrime measures (Model 1), individuals who engage in piracy and those who feel that they should be allowed to access any data anywhere are more willing to engage in defacements. In the political model (Model 2), those who are supportive of outgroup antagonism and are willing to perform multiple forms of political protest in the real world were more willing to engage in a defacement. In the combined model, piracy and outgroup antagonism are no longer significant (see Model 3). Attitudes toward being able to see any data and engage in protest behaviors remain significant predictors for engaging in defacements.

In the model for defacements against Bagaria, there are generally few significant predictors across the models (see Table 8.2, Models 4–6). In the cybercrime-only model, males are more willing to engage in defacements (see Model 4). In the political model, those who support outgroup antagonism and are willing to engage in multiple forms of political protest are more likely to engage in defacements (see Model 5). In the full model, those who felt that there are no clear rules regarding ethical behavior online were more likely to engage in defacements (see Model 6). This variable was non-significant in the previous model, while outgroup antagonism became non-significant. Physical protest behaviors remained significant, as did gender. Thus, in comparing Models 1 through 3 with 4 through 6, there appear to be some differences in the correlates of foreign and domestic targets.

The models for searching government servers for sensitive papers (see Table 8.3) share some similarities to the correlates for defacements. The cybercrime-only model for domestic targets shows that those who spend more time online, engage in piracy, and feel they should be able to access any data maintained are more willing to search servers (see Model 1). In the political model, those who are have antagonistic attitudes toward marginalized groups and are willing to engage in multiple forms of physical protest are more likely to search servers for information (see Model 2). The combined model shows that the significant variables from the cybercrime-only model remain significant, though outgroup antagonism becomes non-significant (see Model 3). In addition, Taiwanese respondents are more willing to engage in this behavior.

The Bagarian targeting models (see Models 4–6) share many of the same relationships as the domestic model. In the cybercrime-only model, those who feel they should be able to access data and those who do not think that law enforcement is quick to recognize when cybercrimes occur were more willing to engage in attacks (see Model 4). In addition, Taiwanese respondents were more willing to engage in this form of attack. In the political model, outgroup antagonism and physical protest behaviors were significant again (see Model 5). The relationships observed in the combined model are quite similar to that of the domestic targeting model. Specifically, spending more time online, maintaining a belief that you should be able to look at any data, engaging in multiple forms of physical protest and being from Taiwan were all significant correlates of willingness to search Bagarian servers (see Model 6).

The correlates for individual willingness to compromise military servers are quite similar to that of searching government servers across both the domestic and Bagarian models (see Table 8.4). In the domestic model with cybercrime variables only, those who spend more time online and do not think law enforcement recognizes when cybercrime occurs were more willing to engage in this behavior (see Model 1). In the political model, outgroup antagonism and physical protest behaviors are significantly correlated with willingness to compromise military servers (see Model 2). In the combined model, time online becomes non-significant, though all other relationships remain significant (see Model 3).

The correlates for willingness to attack Bagarian targets are somewhat similar to the domestic targeting variables. In the cybercrime model, those who do not think law enforcement recognize cybercrimes and respondents from Taiwan were more likely to engage in this behavior (see Model 4). Outgroup antagonism and physical protest behaviors were significant predictors in the political model (see Model 5). In the combined model, only attitudes toward law enforcement, physical protest behaviors and respondents from Taiwan were predictors of being likely to engage in military server compromises (see Model 6). Due to the extremely small proportion of respondents who were willing to engage in this behavior, an ROC model was generated to assess the accuracy of these findings. The area under the curve was 0.853 (sig. = 0.000), suggesting that this model is able to correctly and with good accuracy classify those willing to engage in attacks (Pencina *et al*., 2008).

Discussion and conclusion

Though there is a substantial amount of research on real-world terror, there is much less research on the correlates of cyberterror, or politically-motivated attacks against online infrastructure (Denning, 2011; Holt and Kilger, 2012; Kilger, 2011). The evolution of technology has made it possible for civilians to easily engage in attacks against government and industry targets online, making them so-called "civilian cyberwarriors" (Denning, 2011; Holt and Kilger, 2012; Kilger, 2011). This study utilized a sample of respondents from the US and Taiwan using a scenario measure for web defacements, searching servers for information, and compromising military servers in order to identify any correlates for action as a cyberwarrior.

The findings suggest that technological skill and involvement in cybercrime behaviors may be less relevant predictors for cyberattack than hypothesized (Correll, 2010; Poulsen, 2011). Participation in digital piracy was only significant in the cybercrime-related variable models and was non-significant in the full models across all forms of attack and targets. Given that technological skill and time online were also non-significant, it appears that individuals do not necessarily need to be technologically proficient in order to pursue politically motivated attacks (Holt and Kilger, 2012).

Table 8.3 Binary logistic regression models for searching government servers ($n = 774$)

	Domestic			*Bagaria*		
	Model 1	*Model 2*	*Model 3*	*Model 4*	*Model 5*	*Model 6*
Variables						
Time online	0.263**	–	0.216*	0.197*	–	0.179*
	(0.099)		(0.106)	(0.091)		(0.094)
Computer skill	0.022	–	0.016	0.021	–	0.018
	(0.022)		(0.023)	(0.020)		(0.021)
Piracy	0.096*	–	0.075	0.034	–	0.015
	(0.048)		(0.052)	(0.045)		(0.047)
Hacking	−0.024	–	−0.060	0.108	–	0.084
	(0.093)		(0.100)	(0.079)		(0.080)
Ethics	−0.198	–	−0.211	0.141	–	0.107
	(0.135)		(0.146)	(0.126)		(0.132)
People allowed	0.024	–	0.058	−0.280	–	−0.303
	(0.190)		(0.199)	(0.190)		(0.198)
I should be able	0.370**	–	0.325*	0.401**	–	0.375**
	(0.136)		(0.144)	(0.130)		(135)
Law enforcement quick	−0.104	–	0.042	−0.361*	–	−0.276
	(0.161)		(0.175)	(0.148)		(0.161)
Hacking not a crime	−0.062	–	−0.045	−0.061	–	−0.054
	(0.164)		(0.173)	(0.153)		(0.161)
Patriotism	–	−0.045	−0.021	–	−0.040	−0.027
		(0.035)	(0.038)		(0.033)	(0.035)

Nationalism	–	−0.090	−0.083	–	−0.070	−0.045
		(0.072)	(0.078)		(0.062)	(0.067)
Group equality	–	0.054	0.037	–	−0.009	−0.019
		(0.042)	(0.044)		(0.036)	(0.039)
Outgroup antagonism	–	0.183***	0.084	–	0.133***	0.039
		(0.041)	(0.057)		(0.035)	(0.051)
Physical actions, homeland	–	0.708***	0.783***	–	–	–
		(0.097)	(0.113)			
Physical actions, Bagaria	–	–	–	–	0.548***	0.555***
					(0.086)	(0.094)
US	−0.160	–	−1.176*	−0.861**	–	−1.232**
	(0.318)		(0.530)	(0.310)		(0.445)
Gender	−0.180	–	−0.155	−0.427	–	−0.359
	(0.265)		(0.289)	(0.248)		(0.261)
Constant	−3.862***	−5.162***	−5.330***	−3.144***	−2.896**	−2.845*
	(0.912)	(1.267)	(1.661)	(0.845)	(1.060)	(1.440)
Model χ^2	32.927***	68.293***	93.793***	45.054***	50.909***	82.944***
R^2	0.085	0.171	233	0.105	0.116	0.189

Notes
Unstandardized coefficients are presented with standard errors in parentheses due to space limitations; *$p<0.05$; **$p<0.01$. ***$p<0.001$. Pseudo R^2 are Nagelkerke R^2.

Table 8.4 Binary logistic regression models for compromising military servers ($n = 774$)

	Domestic			*Bagaria*		
	Model 1	*Model 2*	*Model 3*	*Model 4*	*Model 5*	*Model 6*
Variables						
Time online	0.358*	–	0.287	−0.189	–	0.171
	(0.156)		(0.170)	(0.106)		(0.111)
Computer skill	0.013	–	0.003	0.007	–	0.002
	(0.032)		(0.036)	(0.023)		(0.025)
Piracy	0.099	–	0.073	0.062	–	0.049
	(0.071)		(0.079)	(0.052)		(0.055)
Hacking	0.150	–	0.137	0.135	–	0.121
	(0.115)		(0.125)	(0.085)		(0.088)
Ethics	0.190	–	0.129	0.110	–	0.026
	(0.202)		(0.224)	(0.144)		(0.152)
People allowed	0.390	–	0.440	−0.226	–	−0.170
	(0.262)		(0.288)	(0.218)		(0.288)
I should be able	−0.130	–	–257	0.235	–	0.181
	(0.206)		(0.230)	(0.151)		(0.158)
Law enforcement quick	–790**	–	−0.671*	−0.524**	–	−0.453*
	(0.266)		(0.293)	(0.177)		(0.189)
Hacking not a crime	−0.127	–	−0.090	0.133	–	0.160
	(0.241)		(0.266)	(0.172)		(0.183)
Patriotism	–	−0.053	−0.006	–	0.016	0.054
		(0.052)	(0.061)		(0.039)	(0.044)

Nationalism	–	−0.037	−0.037	–	−0.091	−0.078
		(0.712)	(0.109)		(0.072)	(0.080)
Group equality	–	0.042	0.037	–	−0.054	−0.072
		(0.061)	(0.069)		(0.042)	(0.046)
Outgroup antagonism	–	0.250***	0.211*	–	0.175***	0.067
		(0.060)	(0.085)		(0.041)	(0.059)
Physical actions, homeland	–	0.975***	1.036***	–	–	–
		(0.141)	(0.168)			
Physical actions, Bagaria	–	–	–	–	0.663***	0.651***
					(0.098)	(0.108)
US	0.453	–	−0.180	−0.767*	–	−1.158*
	(0.448)		(0.779)	(0.354)		(0.513)
Gender	−0.207	–	−0.022	−558*	–	−0.423
	(0.387)		(0.437)	(0.291)		(0.310)
Constant	−5.114***	−7.545***	−9.147***	−3.101***	−4.091***	−3.646*
	(1.321)	(1.932)	(2.773)	(0.962)	(1.255)	(1.728)
Model χ^2	26.135**	64.567***	81.830***	38.471***	61.509***	83.273***
R^2	0.110	0.253	0.331	0.106	0.161	0.222

Notes
Unstandardized coefficients are presented with standard errors in parentheses due to space limitations; *$p<0.05$; **$p<0.01$. ***$p<0.001$. Pseudo R^2 are Nagelkerke R^2.

Instead, individuals must be willing to express themselves in an online space and be willing to violate legal conventions in support of their agenda. The significance of the attitudinal measures that support offending behaviors reinforces this concept, though these measures are derived from research on cybercrime rather than on extremist activities (Holt *et al*., 2010; Skinner and Fream, 1997). Those who feel they should be allowed to view any materials available online were more likely to engage in web defacements targeting their home country and were willing to search servers for papers and documents that could embarrass the government. Those who believe that law enforcement does not recognize when cybercrime takes place reported a willingness to compromise military servers. This may be because they feel their risk of detection is low, thereby making it easier to offend. Thus those with attitudes supportive of crime and deviance may be more likely to engage in cyberattacks generally. In turn, we may see an increase in the number of cyberwarriors in the future due to the perceived reduced risk of detection.

Nationalism and patriotism had no demonstrable influence on willingness to engage in cyberattacks (see also Holt and Kilger, 2012). While expressions of nationalism and patriotism are overt in the United States, these attitudes in Taiwan may be more covert due to the serious and sensitive relationship between Taiwan and the Peoples' Republic of China (Putnam, 2000). Additional statistical modelling is necessary to better examine the interaction between country of origin, social factors, and willingness to engage in cyberattacks.

Individuals who do not support the suppression of minority and out-groups in society were more willing to engage in multiple forms of cyberattacks against their home nation. Support for antagonistic relationships appears to influence multiple cyber actions within one's home country. This result is in line with mounting evidence regarding the emergence of online hacktivism in support of marginalized groups and ethnic minorities who may be discriminated against by both internal and foreign sources (Brenner, 2008; Denning, 2011; Holt, 2009; Kilger, 2011; Woo *et al*., 2004). Thus the role of social attitudes may vary in virtual space in line with the larger literature on the contextual nature of violence and terror (Gurr, 1970; LaFree and Dugan, 2009; Martin, 2006; Taylor, 1993).

The most significant political factor across all of these models was the number of attacks an individual was willing to perform in the real world. These findings clearly illustrate that willingness to engage in violence in support of political action cuts across the digital divide (see also Holt and Kilger, 2012). An individual willing to commit an act of violence against a target in cyberspace may also be willing to engage in protest behaviors and physical attacks in the real world. This has particular salience for law enforcement and intelligence agencies, as it suggests that an increase in cyberattacks may be congruous with an increased potential for physical attacks. Should they occur in tandem, then a much more serious set of negative outcomes may result for the target and the citizens of that nation (Ayers, 1999; Brenner, 2008; Denning, 2011; Earl and Schussman, 2003). In addition, the strong relationship between intention to commit physical and cyberattacks in this study may reflect the value in exploring an individual's propensity to engage in attacks in both virtual and real environments.

There were also differences in individual action based on the country where this data was collected. Respondents from Taiwan were more likely to choose the options to search servers for embarrassing papers and compromise military servers. This difference may stem from Taiwan's proximity to China, where politically motivated hacking against foreign targets is extremely common and accepted (Brenner, 2008). This may increase the willingness of individuals, particularly technologically savvy youth, to engage in cyberattacks against various targets relative to those in the US. Further research is needed to clarify the macro- and micro-level factors unique to a given nation that affect willingness to engage in attack (Holt and Kilger, 2012; Stepanova, 2011).

Additional research is also necessary to expand the limited generalizability of these findings beyond the present study. Developing samples from diverse groups within the general public, such as older individuals and those living in poverty, may help to clarify how economic conditions or exposure to technology influence willingness to engage in political violence on- and offline.

It is also critical to note that the respondents in this sample who reported a willingness to engage in cyberattacks may not actually act on these feelings in the future. Research on physical terrorism and political violence indicates that a very small proportion of individuals are radicalized to violent actions over time, and even fewer actually engage in violence at any point (Moskalenko *et al*., 2010). The process of radicalization can vary, and it involves social, economic and individual drivers that may be unique to an area or circumstance (McCauley and Moskalenko, 2008). The same may be true regarding cyberattacks, though there is scant research that considers these issues or provides direction for policy-makers. Though this exploratory analysis provides some insights regarding the predictors for political action against both foreign and domestic targets, the large number of non-significant variables suggests there is a need for more refined theoretical frameworks to assess predictors for cyberattacks. Additional studies are needed, and may benefit from incorporating variables and theoretical models from the radicalization literature to improve our knowledge of virtual political expression. In turn, we may be able to clarify the relationship between extremist behaviors on- and offline, and any variations in the predictors for political violence overall.

Notes

1 The term "defacement" was not defined for respondents.
2 Respondents were not informed that Bagaria was a fictitious country, as it was thought that respondents would either recognize this on their own or assume that it was a place they had not heard of before. This is appropriate as it provides a mechanism to avoid individual respondent biases which may otherwise exist.
3 Respondents were asked two separate questions regarding Unix or Linux in order to capture differential exposure and experience with the software. For instance, an individual may have used a Unix or Linux system during a course or through an acquaintance, while the installation of this software is a different but related activity. This was evident in the fact that these items were correlated, but not perfectly ($r = 0.631$**).

References

Akers, Ronald L. (1998) *Social Learning and Social Structure: A General Theory of Crime and Deviance*. Boston: Northeastern University Press.

Al-Rizzo, H. M. (2008) The undeclared cyberspace war between Hezbollah and Israel. Contemporary Arab Affairs. 1, pp. 391–405.

Andress, J. and Winterfeld, S. (2011) *Cyber Warfare: Techniques, Tactics, and Tools for Security Practitioners.* Waltham MA: Syngress.

Ayres, J. M. (1999) From the streets to the Internet: The cyber-diffusion of contention. *The Annals of the American Academy of Political and Social Science*. 566, pp. 132–143.

Bossler, A. M. and Burruss, G. W. (2011) The general theory of crime and computer hacking: Low self-control hackers? In Holt, T. J. and Schell, B. H. (eds) *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications.* Hershey PA: IGI Global.

Bossler, A. M. and Holt, T. J. (2010) The effect of self-control on victimization in the cyberworld. *Journal of Criminal Justice*. 38 (3), pp. 227–236. Doi: 10.1016/j.jcrimjus.2010.03.001.

Brenner, S. W. (ed.) (2008) *Cyberthreats: The Emerging Fault Lines of the Nation State.* New York: Oxford University Press.

Brewer, M. B. (1999) The psychology of prejudice: Ingroup love or outgroup hate? *Journal of Social Issues*. 55, pp. 429–444.

Brodscky, J. and Radvanovsky, R. (2011) Control systems security. In Holt, T. J. and Schell, B. (eds) *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications.* Hershey PA: IGI-Global.

CIA (Central Intelligence Agency) (2013) *The World Factbook 2013–14*. Central Intelligence Agency.

Chermak, S., Freilich, J. and Suttmoeller, M. (2013) The organizational dynamics of far-right hate groups in the United States: Comparing violent to non-violent organizations. *Studies in Conflict and Terrorism.* 36, pp. 193–218.

Chu, B., Holt, T. J. and Ahn, G. J. (2010) *Examining the Creation, Distribution, and Function of Malware On-line.* Washington DC: National Institute of Justice. Available at: www.ncjrs.gov./pdffiles1/nij/grants/230112.pdf. Accessed 15 June 2011.

Conover, P. J., Searing, D. D. and Crewe, I. (2004) The elusive ideal of equal citizenship: Political theory and political psychology in the United States and Great Britain. *Journal of Politics*. 66 (4), pp. 1036–1068.

Correll, S. P. (2010) An interview with Anonymous. *PandaLabs Blog.* Available at: http://pandalabs.pandasecurity.com/an-interview-with-anonymous/. Accessed 1 August 2012.

Curtin, R., Presser, S. and Singer, E. (2005) Changes in telephone survey non-response over the past quarter century. *Public Opinion Quarterly*. 69, pp. 87–98.

Dalton, R. (ed.) (2002) *Citizen Politics: Public Opinion and Political Parties in Advanced Institutional Democracies*. 3rd edn. Chatham NJ: Chatham House Publishers.

Denning, D. E. (2011) Cyber-conflict as an emergent social problem. In Holt, T. J. and Schell, B. (eds) *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications.* Hershey PA: IGI-Global.

Dillman, D. A. (ed.) (2007) *Mail and Internet Surveys: The Tailored Design Method.* Hoboken NJ: John Wiley and Sons, Inc.

Duckitt, J. (2003) Prejudice and intergroup hostility. In Sears, D. O., Huddy, L. and Jervis, R. (eds) *Oxford Handbook of Political Psychology*. New York: Oxford University Press.

Earl, J. and Schussman, A. (2003) The new site of activism: On-line organizations, movement entrepreneurs and the changing location of social movement decision-making. In Coy, P. G. (ed.) *Consensus Decision Making, Northern Ireland and Indigenous Movement*s. London: JAI Press.

Fan, W. and Yan, Z. (2010) Factors affecting response rates of the web survey: A systematic review. *Computers in Human Behaviour*. 26, pp. 132–139.

Fishbein, M. J. and Ajzen, I. A. (eds) (1975) *Belief, Attitude, Intention, and Behaviour: An Introduction to Theory and Research.* Reading MA: Addison Wesley Publishing.

Friedkin, N. E. (2004) Social cohesion. *Annual Review of Sociology.* 30, pp. 409–425.

Gruenewald, J., Chermak, S. and Freilich, J. (2013) Distinguishing loner attacks from other domestic extremist violence: A comparison of far-right homicide incident and offender characteristics. *Criminology and Public Policy*. 12, pp. 65–91.

Gurr, T. R. (1970) *Why Men Rebel.* Princeton NJ: Princeton University Press.

Herrmann, R. K., Tetlock, P. E. and Visser, P. S. (1999) Mass public decisions to go to war: A cognitive-interactionist framework. *The American Political Science Review*. 93, pp. 553–573.

Higgins, G. E. (2005) Can low self-control help with the understanding of the software piracy problem? *Deviant Behaviour.* 26, pp. 1–24.

Higgins, G. E. and Wilson, A. L. (2006) Low self-control, moral beliefs, and social learning theory in university students' intentions to pirate software. *Security Journal*. 19, pp. 75–92.

Hinduja, S. (2001) Correlates of Internet software piracy. *Journal of Contemporary Criminal Justice*. 17, pp. 369–382.

Holt, T. J. (2009) The attack dynamics of political and religiously motivated hackers. In Saadawi, T. and Jordan, L. (eds) *Cyber Infrastructure Protection.* New York: Strategic Studies Institute.

Holt, T. J. and Kilger, M. (2012) Examining willingness to attack critical infrastructure in and off-line. *Crime and Delinquency*. 58, pp. 798–822.

Holt, T. J., Burruss, G. W. and Bossler, A. M. (2010) Social learning and cyber deviance: Examining the importance of a full social learning model in the virtual world. *Journal of Crime and Justice*. 33, pp. 31–62.

Huddy, L. and Khatib, N. (2007) American patriotism, national identity, and political involvement. *American Journal of Political Science*. 51, pp. 63–77.

Ingram, J. and Hinduja, S. (2008). Neutralizing music piracy: An empirical examination. *Deviant Behavior*. 29 (4), pp. 334–366. Doi: 10.1080/01639620701588131.

Jennings, K. M. and Zeitner, V. (2003) Internet use and civic engagement: A longitudinal analysis. *Public Opinion Quarterly.* 67, pp. 311–334.

Jordan, T. and Taylor, P. (eds) (2004) *Hacktivism and Cyber Wars.* London: Routledge.

Kilger, M. (2011) Social dynamics and the future of technology-driven crime. In Holt, T. J. and Schell, B. (eds) *Corporate Hacking and Technology Driven Crime: Social Dynamics and Implications*. Hershey PA: IGI-Global.

Kim, M. S. and Hunter, J. E. (1993) Relationships among attitudes, behavioural intentions, and behaviour: A meta-analysis of past research Part 2. *Communications Research.* 20, pp. 331–364.

Kosterman, R. and Feshbach, S. (1989) Toward a measure of patriotic and nationalistic attitudes. *Political Psychology*. 10, pp. 257–274.

Kunovich, R. M. and Hodson, R. (1999) Conflict, religious identity, and ethnic intolerance in Croatia. *Social Forces*. 78, pp. 643–668.

LaFree, G. and Dugan, L. (2009) Research on terrorism and countering terrorism. *Crime and Justice.* 38, pp. 413–477.

LaFree, G., Yang, S. M. and Crenshaw, M. (2009) Trajectories of terrorism: Attack patterns of foreign groups that have targeted the United States, 1970 to 2004. *Criminology and Public Policy.* 8, pp. 445–473.

Lavis, J. and Stoddart, G. (2003) Social cohesion in health. In Osberg, L. (ed.) *The Economic Implications of Social Cohesion*. Toronto: University of Toronto Press.

Martin, G. (ed.) (2006) *Understanding Terrorism: Challenges, Perspectives, and Issues*. 2nd edn. Thousand Oaks CA: Sage.

Maruna, S., and Copes, H. (2005) What have we learned in five decades of neutralization research? Crime and Justice. 32, pp. 221–320.

McCauley, C. and Moskalenko, S. (2008). Mechanisms of political radicalization: Pathways toward terrorism. *Terrorism and Political Violence*. 20 (3), pp. 415–433. Doi: 10.1080/09546550802073367.

Moskalenko, S., Hataley, T., Leuprecht, C. and McCauley, C. (2010) Containing the narrative: Strategy and tactics in countering the storyline of global Jihad. *Journal of Policing, Intelligence and Counter Terrorism*. 5 (1), p. 42. Doi: 10.1080/18335300.2010.9686940.

Mummendey, A., Klink, A. and Brown, R. (2001) Nationalism and patriotism: National identification and out-group rejection. *British Journal of Social Psychology*. 40, pp. 159–172.

Nagin, D. and Paternoster, R. (1993) Enduring individual differences and rational choice theories of crime. *Law and Society Review*. 27, pp. 467–496.

Payne, B. K. and Chappell, A. (2008) Using student samples in criminological research. *Journal of Criminal Justice Education.* 19, pp. 175–192.

Pencina, M. J., D'Agostino, R. B. and Vasan, R. S. (2008) Evaluating the added predictive ability of a new marker: From area under the ROC curve to reclassification and beyond. *Statistics in Medicine*. 27, pp. 157–172.

Pettigrew, T. F. (2003) Peoples under threat: Americans, Arabs, and Israelis. *Peace and Conflict: Journal of Peace Psychology.* 9, pp. 69–90.

Piquero, A. R. and Bouffard, J. A. (2007) Something old, something new: A preliminary investigation of Hirschi's redefined self-control. *Justice Quarterly*. 24, pp. 1–27.

Post, J. M. (1998) Terrorist psycho-logic: Terrorist behaviour as a product of psychological forces. In Reich, W. (ed.) *Origins of Terrorism: Psychologies, Ideologies, Theologies, States of Mind*. Washington DC: Woodrow Wilson Center.

Poulsen, K. (2011) *Kingpin: How One Hacker Took Over the Billion-Dollar Cybercrime Underground*. New York: Crown.

Putnam, R. D. (ed.) (2000) *Bowling Alone: The Collapse and Revival of American Community.* New York: Simon and Schuster.

Schatz, R. T. and Staub, E. (1997) Manifestations of blind and constructive patriotism: Personality correlates and individual group relations. In Bar-Tal, D. and Staub, E. (eds) *Patriotism in the Lives of Individuals and Nations*. Chicago: Nelson-Hall Publishers, pp. 229–246.

Schatz, R. T., Staub, E. and Lavine, H. (1999) On the varieties of national attachment: Blind versus constructive patriotism. *Political Psychology*. 20, pp. 151–174.

Schmid, A. P. (ed.) (1988) *Political Terrorism.* Amsterdam: North Holland Press.

Schmid, A. P. (2004) Frameworks for conceptualising terrorism. *Terrorism and Political Violence*. 16, pp. 197–221.

Schussman, A. and Soule, S. A. (2005) Process and protest: Accounting for individual protest participation. *Social Forces*. 84, pp. 1083–1108.

Sheehan, K. B. (2001) E-mail survey response rates: A review. *Journal of Computer-Mediated Communication*, 6 (2).

Sibley, C. G., Robertson, A. and Wilson, M. S. (2006) Social dominance orientation and right wing authoritarianism: Additive and interactive effects. *Political Psychology*. 27, pp. 755–768.

Sidanius, J. and Pratto, F. (ed.) (2001) *Social Dominance: An Intergroup Theory of Social Hierarchy and Oppression*. Cambridge: Cambridge University Press.

Sifry, M. (ed.) (2011) *WikiLeaks and the Age of Transparency.* New York: OR Books.

Skinner, W. F. and Fream, A. M. (1997) A social learning theory analysis of computer crime among college students. *Journal of Research in Crime and Delinquency*. 34, pp. 495–518.

Stepanova, E. (2011) The role of information communications technology in the "Arab Spring": Implications beyond the region. PONARS Eurasia Policy Memo No. 159. Available at: www.gwu.edu/~ieresgwu/assets/docs/ponars/pepm_159.pdf. Accessed 20 August 2012.

Sykes, G. M. and Matza, D. (1957) Techniques of neutralization: A theory of delinquency. *American Sociological Review*. 22 (6), pp. 664–670.

Taylor, P. (ed.) (1993) *States of Terror: Democracy and Political Violence.* London: Penquin.

Terry, D. J., Hogg, M. A. and Duck, J. M. (1999) Group membership, social identity, and attitudes. In Abrams, D. and Hogg, M. A. (eds) *Social Identity and Cognition*. Oxford: Blackwell Publishers.

Van Evera, S. (1994) Hypotheses on nationalism and war. *International Security*. 18, pp. 5–39.

Van Laer, J. (2010) Activists online and offline: The Internet as an information channel for protest demonstrations. *Mobilization: An International Journal*. 15, pp. 347–366.

Vasi, I. B. (2006) The new anti-war protests and miscible mobilizations. *Social Movement Studies*. 5, pp. 137–153.

Verba, S., Schlozman, K. L. and Brady, H. (eds) (1995) *Voice and Equality: Civic Voluntarism in American Politics.* Cambridge MA: Harvard University Press.

Vollhardt, J. K., Migacheva, K. and Tropp, L. R. (2009) Social cohesion and tolerance for group differences. In De Rivera, J. (ed.) *Handbook on Building Cultures of Peace*. New York: Springer.

Wilson, C. (2008) *Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress.* Congressional Research Service Report RL32114.

Wiltfang, G. and McAdam, D. (1991) Distinguishing cost and risk in sanctuary activism. *Social Forces.* 69, pp. 987–1010.

Woo, H., Kim, Y. and Dominick, J. (2004) Hackers: Militants or merry pranksters? A content analysis of defaced web pages. *Media Psychology*. 6, pp. 63–82.

This page intentionally left blank

Part II

Counter-terrorism

Prospects, pitfalls, policies

This page intentionally left blank

9 Security networks and counter-terrorism

A reflection on the limits of adversarial isomorphism

Benoît Dupont

For many observers the attacks of 11 September 2001 confirmed the dawn of a "new" terrorism: one that would distinguish itself from conventional forms of political violence by its advanced degree of decentralization. The "old" ideological terrorism, organized under a traditional hierarchy, with a political agenda and a readiness to claim responsibility for its actions, has allegedly been replaced with a terrorism characterized by mystico-religious motivations justifying catastrophic consequences, prepared to use weapons of mass destruction, and operating under a decentralized structure. The pyramidal terrorist organization, which mirrors military command principles, would be transformed into a distributed structure capable of enduring repeated attacks and operating even when its "control center" is temporarily or definitively weakened (Gunaratna, 2004; Hoffman, 2006; Jurgensmeyer, 2000; Laqueur, 1999; Lesser *et al*., 1999).

However, as Maurice Roche so well put it, "without memory, everything is new." Whether it is the anarchist wave that fell upon Europe and North America at the end of the nineteenth century, the Algerian terrorism that spurred Algeria's decolonization during the 1960s, or the Vietcong guerrillas, all of these movements had networks that operated in a way that challenged the large hierarchical state structures battling them (Deflem, 2002; van Meter, 2002). Charles Tilly (2005) demonstrated how for several centuries "trust networks" have enabled ethnic and religious minorities to guard against the "malfeasance, mistakes and failures" of their members, allowing them to endure hostile political and economic environments. Manuel Castells (2000) further highlighted the important role social and organizational networks played across different periods, regions and cultures. The use of this social morphology as a variable to explain the "new" terrorism therefore seems rather abusive.

In this context, two complementary factors seem to help explain the renewed interest in terrorist networks. The first factor is related to the remarkable progress made over the last 20 years by technical and information networks, profoundly altering the relationship of social networks to time and space. As with many other areas of human activity, terrorist groups have learned how to use the potential of the Internet and the latest means of communication to securely exchange information, spread propaganda, recruit members from across the world, and provide distance training on terrorism

tactics (Weimann, 2006). This "Jihad 2.0" (Labi, 2006) is not as much a description of a transition to the highly proclaimed cyberterrorism as much as it is the emergence of an increased effectiveness of weakly connected networks, which were previously restricted by major geographical barriers. This convergence between technical and social networks is in the process of generating a new institutional ecology, particularly useful for non-state and non-commercial actors (Benkler, 2006).

The second factor is also technological in nature, but without the same degree of structural complexity as the first. Recent years have seen an increase in the number of computerized visualization tools enabling users to observe complex social, geographical and temporal relationships through images. This innovation, credited to the enhanced power of computing tools and greater number of databases, has had a huge impact on most security organizations, whether they are police forces or intelligence agencies (Klerks, 2001). Computer programs such as the Analyst's Notebook (marketed by i2, a division of IBM), Xanalys, Maltego (marketed by Paterva), and many others produce diagrams covered in arrows connecting symbols of known terrorists and their suspicious associates with places, devices (such as mobile phones), bank accounts, IP addresses etc. (Xu and Chen, 2005). These visual representations of complex social and technical "Dark networks" (Raab and Milward, 2003) have worked their way into pop culture through intelligence TV shows and movies such as *24*, *Homeland* and *Zero Dark Thirty*.

Even if these precious tools help visualize patterns and connections not easily detectable in the thousand-page narrative reports generated by security organizations every day, they also considerably reduce the information analyzed in a binary classification between, on one hand, individuals suspected through association, and on the other hand, those who benefit from temporary get-out-of-jail-free cards as long as their names are absent from terrorism databases. The visual appeal of this kind of imagery is so alluring that a late American artist used it as his favorite way of expressing himself. This was a rare instance where national security and a gallery owner collaborated on a case. One of the artist's works was used by the FBI in their investigation of the 9/11 attacks (Hobbs, 2003). In this case, taking the saying "a picture is worth a thousand words" literally brings to mind a few paradoxes concerning the anti-terrorism fight: an analyst's capacity to reflect and conceptualize can be negatively affected by how the information is graphically formatted, in a field where ambiguity and uncertainty play an important role in understanding a fluid reality (Tufte, 1990).[1]

The first section of this chapter will deal with the new counter-terrorism orthodoxy and the three types of responses that government authorities have developed to address contemporary terrorist phenomena. The first response consists in using the knowledge available on the structure of terrorist networks to destabilize and weaken them. The second, a more radical response, urges public authorities to take stock of the superiority of networks over bureaucracies and encourages them to transform their vertical structures into horizontal

institutions. The second response gives rise to the third: an acceleration of the hybridization between—typically segmented—sectors involved in the fight against terrorism. This isomorphic strategy appears to us, however, to largely underestimate the profound differences that distinguish terrorist networks from administrative and organizational networks. In the second section of this chapter, I outline three paradoxes—of trust, information and legality—that explain why the mimicry strategy appears to be flawed. The trust paradox reflects the fact that while cohesive terrorist networks can leverage "resilient trust," heterogeneous organizational networks are rarely able to move beyond a fragile kind of trust that makes collaboration more contingent. The information paradox shows how the network form of organization, instead of making the acquisition and processing of information more effective, makes available vast quantities of data that are not always relevant to the needs of network members, forcing them to develop coping strategies that often produce undesirable outcomes. Finally, the legality paradox examines the tension between the effectiveness offered by the network form of organization and the procedural fairness and accountability mechanisms that counter-terrorism bureaucracies must uphold in liberal democracies.

Networks versus networks: the response of public institutions

Three types of responses that are advocated against emerging terrorist networks are said to possess a competitive advantage over segmented government bureaucracies filled with excessively rigid procedures. The first response consists of identifying the structural vulnerabilities of the terrorist network and concentrating anti-terrorist efforts on exploiting these weaknesses to disable its structure. This was the preferred response by security services on several occasions in the 1950–70 decolonization insurgency battles, as well as more recently in Northern Ireland (van Meter, 2002). This response has gained popularity due to advances in research on social networks. The second response aims less at fighting terrorist networks directly and focuses more on having public security organizations catch up with the network form of organization. This idea, put forth mainly by researchers affiliated with military or private think tanks, quickly gained popularity due to the numerous institutional failures brought to light by the various committees that analyzed the lessons taken from 9/11. This tendency is not confined to the anti-terrorism sphere; it has been a topic of interest for several years now on a much larger stage—public administration as a whole (Lowndes and Skelcher, 1998). In parallel with the ambitious objective of thoroughly revising the state's intervention methods, a third category of transformation must be examined, that of an accelerating hybridization process between public and private actors playing a role in the fight against terrorism. If the last two responses inevitably overlap, the fragmented, non-coordinated and sometimes contradictory nature of the phenomena observed in the third category differs greatly from the unified and rationalized vision in the second, which still remains largely theoretical.

Destabilizing terrorist networks

Although networks have many advantages over centralized organizations, the weak links that provide networks with greater flexibility are also their vulnerability. In the absence of redundant mechanisms and standard operating procedures, the removal of the most important actors and the circulation of false information would have a much greater impact on a network than on a vertically integrated organization. Several destabilizing strategies are possible. After analyzing social networks and determining their key players—who either play a central role or have a greater variety of contacts than their partners, thus allowing their network access to external actors—as well as the relational structure that link them to each other, the weak and strong ties can be manipulated more easily depending on the approach.

The most evident among these approaches consists in neutralizing the members of the network. This should be done in order of importance by compromising the members who have the most impact on the network's effectiveness, its adaptability and the circulation of information among its members (Arkin, 2002). Insider information (whether it is true or false) could be sent to actors known for distributing information throughout the network more quickly than their counterparts. The information could also be sent to actors who will use it for their own personal benefit: for example, to climb the ranks with disregard for how this could harm the network as a whole. In networks with internal conflict, support can be provided to faction and dissident groups (Carley *et al*., 2002). Another tactic consists in overloading terrorist networks with information. This forces network members to verify the credibility of the data, thus making each transaction more costly. It also makes it easier to identify the nodes that communicate the most (Deibert and Stein, 2002).

There are three main criteria for evaluating the success of these strategies. They can be measured with the same social network analysis methods used to diagnose how well networks operate. They are: the reduction in the quantity of information distributed among the members of the network; the increasing difficulty the network has with coming to consensus on decisions; and the difficulties the network encounters with accomplishing tasks or interpreting information provided to it (its effectiveness) (Carley *et al*., 2002). However, modesty in such an undertaking remains essential: the capacity to promptly replace a network's key player is exactly what makes terrorist networks adaptable and resilient. The numerous reports of the capture or execution of Al-Qaeda members in Afghanistan and Iraq did not stop rapid reorganizations and continued attacks (Lewis, 2013; Knoke, 2013). As a Canadian Security Intelligence Service foresight project very aptly stated: "Al-Qaeda's obituary has been written many times before, only to have been proven to be presumptuously wishful thinking" (Canadian Security Intelligence Service, 2013).

Organizational mimicry and horizontal injunction

A few days after the 2001 attacks on New York and Washington, a tactical coalition of journalists, researchers, contractors and senior-level Pentagon officials proclaimed that vertical structures were not effective against "asymmetric" non-state

threats posed by modern terrorist groups. These new organizational missionaries based their conclusion predominantly on John Arquilla and David Ronfeldt's idea of netwar: a doctrine about the polycentric conflict that developed at the Rand Corporation during the 1990s (Arquilla and Ronfeldt, 2001). They advocated, rather explicitly, transforming the military, police and intelligence institutions into networks: the only type of structure capable of overcoming the bureaucratic weight responsible for surprise effects similar to those experienced on 9/11. Arquilla even declared to the *Washington Post*: "It takes a tank to fight a tank. It takes a network to fight a network" (Garreau, 2001). A few months later, a professional publication destined for the US federal public service urged readers to adopt network ways of thinking and taking action (Friel, 2002). But no one has expressed better than General Stanley McChrystal how this idea became the new mantra of military and intelligence leaders in the Global War on Terrorism. In a *Foreign Policy* article published shortly after his retirement, he stated:

> In bitter, bloody fights in both Afghanistan and Iraq, it became clear to me and to many others that to defeat a networked enemy we had to become a network ourselves. We had to figure out a way to retain our traditional capabilities of professionalism, technology, and, when needed, overwhelming force, while achieving levels of knowledge, speed, precision, and unity of effort that only a network could provide.
>
> (McChrystal, 2011)

This organizational revolution, which had been triggered by General Petraeus in late 2006 with the publication of an updated manual on the US Army counterinsurgency doctrine (Knoke, 2013), extends far beyond security agencies and the military. It reflects the disillusionment of the New Public Management vis-à-vis the two other dominant institutional morphologies: the state and the market. Table 9.1, inspired by Rhodes's work on governance (Rhodes, 2006), illustrates the positive aspects attributed to networks (more agile and less restrictive than state structures) and the values they are based on, such as trust and reciprocity, which transcend maximizing profits and fierce competition. Thus networks appear to represent an ideal compromise between bureaucratic efficiency and market diversity.

Table 9.1 Three organizational morphologies

	State	*Market*	*Network*
Basis of relationship	Law	Contract	Resource sharing
Degree of dependency	Dependency	Autonomy	Interdependency
Currency	Authority	Money	Trust
Methods for resolving conflicts and coordinating issues	Rules and instructions	Negotiation and arbitration	Diplomacy and compromise
Culture	Subordination	Competition	Reciprocity

The three morphologies displayed in Table 9.1 clearly describe ideal types that are not found in "pure" form in reality and that, in their diluted form, do not mutually exclude each other. They actually cohabit in an entanglement of contested practices, cultures and rationalities, which makes their implementation difficult, some actors being active in state, market and network structures simultaneously. It still may be too early to conclusively evaluate the efforts made during the past decade to flatten and unify the institutions responsible for leading the fight against terrorism. Nevertheless, several examples of hybridization demonstrating the increased partnerships and the entry of new actors into this field can already be observed.

The acceleration of anti-terrorist hybridizations in a post 9/11 world

The anti-terrorist fight saw the standards and conventions governing how it operates change significantly after 9/11. Although these changes are mainly noticeable in the US, the increased cooperation between services and the influence the US has on its allies as a result will more than likely encourage the spread of these practices in allied countries—the war on drugs is a prime example of this trend in the diffusion of security innovation (Nadelmann, 1997). These changes have produced three types of hybridization. First, the state's monopoly in the fight against terrorism is fading, and the private sector's participation is increasing, not only as a critical infrastructure target to protect but also as a service provider to law enforcement, intelligence and defense agencies. Then, the once impermeable barrier between homeland security and national security has become relatively porous, sometimes to the detriment of basic rights, which were one of the reasons why this partition was built in the first place. Last, the allocation of responsibilities between domestic and international stakeholders is making way for initiatives and partnerships whose implementation transcends traditional categories.

The end of the public–private dichotomy

The destruction of the World Trade Center's twin towers—the former headquarters for many financial institutions—and the attacks on the London Underground and the Madrid railway system demonstrated how critical infrastructures play a vital role in the proper functioning of Western societies, which rely on complex flows of goods, energy and information to sustain themselves. Among these critical infrastructures are industries such as banking, healthcare, energy production, water treatment, and transportation and communication networks. Yet in a context where the welfare state has been replaced by a regulatory state (Braithwaite, 2000), these infrastructures are now owned in large part by the private sector (Government Accountability Office, 2006). As the 9/11 Commission (2004) report highlighted, the first response team that helped evacuate the twin towers was not New York City's police or fire department, it was in fact the building owner's (Silverstein Properties) security agents. In this context, it is

hardly surprising that companies and their private security providers are systematically implicated in prevention initiatives and the fight against terrorism. This type of close collaboration can take on several forms: it can involve coordinating the initial response in the event of an attack; sharing information on potential threats; or even creating and offering training to private security actors (Morabito and Greenberg, 2005).

Data collection and analysis are also areas in which the private sector makes some "major moves." First of all, the Patriot Act, both the initial 2001 version and the subsequent 2006 extended version, considerably strengthened information-sharing mechanisms regarding the personal data of American citizens. The criteria for using National Security Letters (or self-issued subpoenas), which allows one to obtain banking and business information without a warrant, has also been relaxed and was used by the FBI in more than 15,200 instances in 2012 (with a peak of 30,000 requests to Foreign Intelligence Surveillance Court in 2005) (Kadzik, 2013; Nakashima, 2007; Lichtblau and Mazzetti, 2007). The statistics regarding the Pentagon's and the CIA's use of this procedure remains confidential. Even before the deluge of revelations made by Edward Snowden during the summer of 2013 about the massive scale of online surveillance conducted by the National Security Agency (NSA), as well as its symbiotic relationship with large telecommunications and technology companies, a few notorious scandals involving the transfer of massive amounts of information by a first-tier telecommunications company (AT&T), airlines (JetBlue and Northwest) and an international banking consortium (SWIFT) had provided hints of new agreements connecting the private sector with government agencies in the anti-terrorism fight.[2] In Canada, the Customs Act (R.S.C., (1985), c. 1 (2nd Supp.)) and the 2003 Passenger Information (Customs) Regulations give border authorities the right to demand that commercial carriers, travel agents and reservation centers provide them with information about passengers. This data is collected by companies to offer travelers the most personalized and comfortable experience possible, but it indirectly allows governments to keep a much closer eye on travelers than in the past. The data also provides a host of financial, religious and medical information about passengers without any legal oversight. Similar requirements exist for transmitting and declaring information in the banking sector under regulations adopted to fight money laundering and terrorism financing (Amicelle, 2011; Gagnon and Bacher, 2004).

This erosion of the legal boundaries that once restricted the flow of personal information is predominantly a result of the findings made by intelligence, law enforcement agencies, and the think tanks that advise them about the technological advances of data aggregation companies, which have created sophisticated consumer profiling tools used for improving direct marketing campaigns (Markle Foundation Task Force, 2003). Private contractors have also captured a significant share of the US intelligence budget and have developed a multi-billion-dollar market resting on the collection and analysis of massive amounts of data. In the greater Washington DC region, this trend has spawned a sort of Silicon Valley of spies ("Spook Valley"—Murphy, 2001). According to a groundbreaking

investigative report prepared by the *Washington Post*, in September 2010 more than 1,900 corporations provided a broad variety of counter-terrorism services to more than 1,200 government organizations, from satellite to cyberoperations and from human intelligence to disaster preparedness (Priest and Arkin, 2010).

For example, the company Word-Check signed a contract with the Department of Homeland Security (DHS) to have access to a database of over 250,000 individuals and companies deemed "at risk" as a result of direct participation or being in some way linked to a criminal, terrorist or money-laundering outfit. This database is considered to be more comprehensive than the one the DHS possesses currently, mainly due to looser restrictions on inclusion criteria (Lichtblau, 2004). Choicepoint, a data aggregation company mandated by the US Department of Justice, had to explain to the Mexican and Colombian justice departments why it illegally acquired electoral files and personal data on millions of South American citizens (Burkeman and Tuckman, 2003). The data were used by US immigration services and customs, the DEA and the FBI to check the identity of potential suspects. Other companies, such as BAE Systems, CACI and L-3 Communications, also provide the public sector with "turnkey" solutions for gathering, translating and analyzing data. This outsourcing of what appears core intelligence and anti-terrorism functions is not a marginal trend: in May 2007, the accidental release of a Powerpoint presentation prepared for a procurement conference revealed that the US intelligence community was spending 70 percent of its budget on contracts at that time, which amounted to roughly $43.5 billion (Shorrock, 2008).

The unexpected overlap of national security and homeland security

The classical distinction between national and homeland security is fading, threatening the systems that had been put in place to protect the freedoms of citizens—even if these rights were not extended to foreign nationals. In several cases, the legal barriers that had been erected have been rather obviously dismantled. For example, the anti-terrorist bill C-36 adopted by Canada in December 2001 altered the provisions of the national defense act regarding the Communications Security Establishment Canada's (CSEC) mandate. This organization is responsible for collecting foreign electromagnetic data (SIGINT) by intercepting electronic communications. Article 273.64 1.c from the National Defense Act expanded CSEC's mandate to include "technical and operational assistance to federal security and law enforcement agencies, such as the Canadian Security Intelligence Service and the Royal Canadian Mounted Police in the performance of their lawful duties." This new provision extends to police organizations considerable resources that had previously been reserved for spying on foreign governments in the conduct of international relations. While this act specifies that the legal limitations that define federal organizations' activities benefiting from the CSEC's assistance applies to (273.64 3) itself, the US did not take the same precautions. Since 9/11, the NSA has been authorized by

the executive branch to intercept the communications of American residents in violation of the Foreign Intelligence Surveillance Act (FISA) (Risen and Licthblau, 2005). This warrantless surveillance was later authorized in an ongoing manner by the FISA Court under an amendment adopted in 2008, despite clear evidence that the NSA was routinely misleading the FISA Court (Ackerman, 2013). While this was happening, the Pentagon was developing TALON, a database meant to make an inventory of terrorist threats targeting its installations. However, it was discovered that the database contained information about militant pacifists and anti-war protests organized by churches, bookstores and other NGOs (Pincus, 2005). Surveillance activities carried out on national soil by armed forces such as these remind citizens of the abuses committed during the Vietnam War by the FBI and its COINTELPRO project.

These national security incursions on homeland security's terrain are accompanied by a symmetrical trend in which the FBI is known to have recruited informants from foreign countries, thereby encroaching on the CIA's prerogatives (Johnston and Jehl, 2005). A similar trend can be identified in Canada, where the Canadian Security Intelligence Service, which initially operated exclusively within Canadian borders, has now established itself abroad (Brodeur and Dupont, 2006). Unlike public–private partnerships, the relationship between these two spheres remains ambivalent, oscillating between collaboration and competition to assume leadership in the fight against terrorism. The ambiguous attitude of the FBI, which benefited from the data gathered by the US Army in foreign countries (such as Afghanistan and Iraq) while prohibiting its agents from taking part in the most violent interrogations in order to avoid tainting potential criminal proceedings, shows to what extent these hybrid networks challenge the prevailing rationalities of each member.

The "glocalization" of anti-terrorism

The last form of hybridization is characterized by the compression of the local–international continuum in the fight against terrorism. Until 9/11, local and national police organizations, along with their foreign counterparts, had clearly-demarcated responsibilities. Furthermore, it was rare for uniformed police officers, whose daily work is carried out closer to citizens, to routinely be associated with the "high policing" tasks that characterize counter-terrorism (Brodeur, 2010). In the post-9/11 world, new arrangements disregard established geographies and jurisdictions.

Thus, in decentralized North America, municipal police forces that find themselves on the front line of a catastrophic attack on a public transportation network, office, or shopping or entertainment complex have considerably increased their anti-terrorist activities, both in collaboration with national organizations and autonomously. The joint investigation and information exchange teams created in the wake of 9/11 are comprised not only of members from various federal law enforcement agencies but also of representatives from local police organizations. In the US, they are called the Joint Terrorism Task Forces

and arrived on the scene in the early 1980s. These squads increased in numbers from 35 to 103 between 2001 and 2005 (Mueller, 2006). There are also over 70 intelligence fusion centers, operating in 37 states, whose mandate is to bring together numerous agencies from various levels of government in order to share intelligence leads widely and therefore generate more analytically robust law enforcement activities (Taylor and Russell, 2012). Beyond their dubious organizational effectiveness, intelligence fusion centers also raise a number of concerns in terms of mission creep (from counter-terrorism to public-order policing for example) and repeated violations of civil liberties, resulting largely from the absence of adequate oversight mechanisms (Monahan and Palmer, 2009). In Canada, the model for integrated investigation teams, which have been used against organized crime since the early 1990s, was expanded in 2003 to the anti-terrorism fight as Integrated National Security Enforcement Teams were created in Montreal, Ottawa, Toronto and Vancouver (Dupont and Pérez, 2006). These teams are comprised of agents from the main federal enforcement organizations (RCMP, Canadian Border Services Agency, Canadian Security Intelligence Service), as well as officers from provincial and municipal police forces. In addition to these official initiatives, there are informal mechanisms. They reflect the frustration felt by local police with regard to the lack of consideration that the national organizations show them and the sluggish rate at which they receive intelligence. Thus, in 2005, police chiefs from about 15 major North American cities put together a communication network that would short-circuit the federal law enforcement agencies (*Law Enforcement News*, 2005). In an unprecedented decision, the New York City police chief entered into direct competition with his country's national agencies as well by creating his own network of liaison officers based in London, Montreal, Toronto, Tel Aviv, Singapore, and Interpol's headquarters in Lyon. During the Madrid attacks, the New York police claimed to have been the first foreign organization on site (Finnegan, 2005).

Along with redefining the inter-organizational responsibilities between local and international law enforcement, there is a broadening of intra-organizational mandates. As Innes (2006) highlighted, the inability of security services to detect the plans for the 9/11, Madrid and London attacks—which nonetheless unfolded in all three cases over a period of several months and in large part on national territory—brought back into question the profile of the terrorist threat and thereby the traditional distinction between high and low policing. This binary distinction aims to differentiate police functions according to their main beneficiary: the state and citizens respectively. While high policing is mainly concerned with the stability of political institutions, low policing seeks to deliver security on behalf of the people (Brodeur, 2010). Although the fight against terrorism has long been handled exclusively through high policing strategies (at least in democratic societies), the past decade has seen a willingness to include uniformed officers in this battle, especially in the United Kingdom. Thus high policing units would infiltrate terrorist networks by intercepting telephone calls and manipulating informants, while low policing units would leverage the trust placed in the police by

neighborhood residents—whether they be originally from there or immigrants—to identify potential signs of terrorist activity in the community and implement community-led counter-radicalization initiatives (Spalek and Lambert, 2008; Spalek, 2010). Such an approach implies that the trust placed in the police is, by definition, superior to that of the loyalty shown towards members of one's ethnic, religious or political minority. This is far from certain in some disadvantaged and socially disorganized neighborhoods (Thatcher, 2005).

The three forms of hybridization described in the preceding paragraphs are not entirely new. However, we are witnessing a change in the scale and scope of initiatives, making any systematic analysis difficult. This explains why scholarly studies seeking to thoroughly examine these questions are so difficult to conduct, and why investigative journalism can also make a significant contribution to our understanding of these new trends. The leaked information gleaned from the NSA files provided by Edward Snowden to Glen Greenwald, Laura Poitras and Barton Gellman provided a unique glimpse of the inner workings and technical capacities mobilized by US intelligence agencies—in close collaboration with private telecommunication and Internet companies—in the fight against terror. But beyond their journalistic value, a more thorough academic analysis of this material still awaits in order to avoid the distortions that inevitably surface in hastily written pieces that sometimes lack the contextual background developed by counter-terrorism scholars. To return to our argument, the few examples put forth attest that these hybrid arrangements can sometimes be interpreted as an attempt by security institutions to comply with injunctions made by think-tank analysts and defense strategists to embrace the network form of organization. However, in many other instances, they become major contributors to the resistance against a more effective coordination of limited resources. This difficulty in producing the expected outcomes stems from a fundamental error in reasoning: the belief that perfect symmetry exists between the characteristics and rationalities of illicit networks (criminals or terrorists) and institutional networks (counter-terrorism assemblages).

Why all networks are not made equal

The arguments used to promote the superior effectiveness of horizontal organization make claims of consistent characteristics such as trust, a better flow of information, and operating costs that are lower than in vertically integrated structures, whereas many variations can be observed from one network to the next (Morselli, 2007). In the ideal-type comparison offered in Table 9.1, the internal homogeneity of the "network" category is overestimated in order to highlight what distinguishes it from the "market" and "bureaucracy" categories. However, three network paradoxes seem to explain more clearly why certain networked organizational configurations are much more effective than others, according to the social and political context under which they operate. These three paradoxes revolve around themes based on trust, the flow of information, and legality.

The trust paradox

Trust plays an essential role in network operation. It enables links and partnerships to be preserved in space and over time without hierarchies or contracts. Many networks do not require a huge expression of trust to function properly. However, as uncertainty and stakes rise, trust becomes a necessity, offering assurance against the "malfeasance, mistakes and failures" of network members (Tilly, 2005). This aspect of trust led Niklas Luhmann (1979) to define it as a "mechanism for reducing complexity." Trust facilitates collaboration and allows social actors to determine reasonable expectations for their partners' and colleagues' behavior. Trust can also consist of a general attitude towards an individual or institution (the Canadian population trusts the police to prevent terrorist attacks), or more specific relationships (I trust the police because the police officer who helped me last week had a professional attitude). General attitudes are of course forged in part through personal experiences, but also though the larger collective experience.

The relational dimension of trust that is particularly interesting here is that it can itself be conceptualized as a continuum with two extremities: one "strong" or resilient side, and a "fragile" side on the opposite end (Ring, 1996). Resilient trust is based on converging interests, beliefs and standards that ensure its continuity—even in crises. This is the unconditional form of trust, which is the main structure for terrorist groups. Fragile trust, by contrast, is situational; that is to say, it is constantly being reevaluated by the two parties in a relationship in order to minimize opportunistic behavior, which considerably increases the cost of transactions between them. This form of negotiated trust prevails between bureaucratic organizations that are in competition for financial resources and a limited reputational capital. Because of their heterogeneity, anti-terrorist networks, which include national and municipal police forces, intelligence agencies, private security companies and community groups, can only hope to operate on limited reserves of fragile trust, as seen for example in the cases of intelligence fusion centers.

Thus, while the resilient trust of terrorist networks enable them to face and survive constant attacks from hostile law enforcement agencies, the latter have to continually deploy considerable efforts and goodwill to maintain functional partnerships. The relationships between main and peripheral actors, and the management of the misunderstanding and friction derived from them, make fragile trust a limitation rather than a catalyst.

The information paradox

Trust considerably influences the effectiveness of networks by enabling them to acquire, transform and distribute information and knowledge rapidly and more economically, whereas hierarchies depend on strict and redundant procedures to perform the same tasks. Social networks use "strong" ties (between closely linked actors) to filter, validate and interpret information based on common

criteria, and "weak" ties (those that occasionally link more distant actors) to diversify their sources of information and encourage innovation that cannot be born out of a homogeneous context (Granovetter, 1973). Unlike most social networks, anti-terrorist networks are faced with a number of barriers that prevent them from using information as efficiently and effectively as they should. First of all, their members do not have the same privileged access to information, since their various levels of security clearance become true data-sharing obstacles. Anti-terrorist networks also suffer from several organizational pathologies (Sheptycki, 2004). The most problematic is unquestionably their inability to analyze the continuously growing mountains of collected data.

The socio-technical networks involved in the fight against terrorism rely on innovations in computer technology and artificial intelligence, whether they are relational databases or data-mining algorithms, which profile individuals according to their risk score based on statistic models with the aim of "connecting the dots" between individual, locations and seemingly isolated acts. However, the sheer amount of information produced by these automated systems prompted analysts to create new metaphors to outdo the traditional analogy of "trying to find a needle in a haystack" with more visually accurate imagery. They referred to the monumental task as being similar to "trying to drink from a fire hose" or "trying to boil the ocean" (Sheptycki, 2004).

As of 2007, police and intelligence databases in the US were amassing information at a rate of around four petabytes per month, or 200 times the quantity of information held in the US Library of Congress (Dizard, 2005). However, in its constant race for larger data storage capacities, the NSA launched the construction in January 2011 of its largest data center yet, located in the Utah desert. It will consist of four 25,000-square-foot halls housing enough servers to eventually be filled with a yottabyte of data, which amounts to 500 quintillion pages of text (Bamford, 2012).[3] However, the accumulation of such staggering quantities of data has not been matched by similar improvements in the analytical capacities of intelligence agencies. For example, anti-terrorism intelligence often has to be translated to English. Linguists, however, cannot keep up with the quantity of the intercepted information. Thus, in a report, the Inspector General of the US Department of Justice indicated that between 2002 and 2004, the FBI had accumulated more than two million hours of telephone intercepts, 30 percent of which could not be translated due to a lack of resources and therefore had to be erased from outdated computers to make room for more recent recordings. Among these untranslated telephone conversations, it is estimated that there were 123,000 hours of terrorism-related content and 500,000 hours of counter-intelligence-related content (Office of the Inspector General, 2004). In other contexts, there are simply no linguists available to quickly translate phone intercepts that might contain information about forthcoming attacks. In Canada, the commission of inquiry into the Air India bombing discovered, for example, that the British Columbia regional office of the Canadian Security Intelligence Service, which was investigating Sikh extremism, lacked a Punjabi-speaking translator and that phone intercepts of the

primary suspect for this attack, who was under surveillance, had to be sent to Ottawa for processing. However, even in Ottawa, the translating resources in that language were so scarce that a significant backlog had accumulated for months on the eve of the bombing (Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182, 2010).

Finally, a more comical example of this information overload has to do with the National Security Agency. In early 2007, the Agency had to alternate between its existing supercomputers and was forced to considerably cut back on purchasing new supercomputers due to the fact that the local electrical company that served its headquarters could not meet the agency's energy needs (Gorman, 2007). In other words, all the electronic data stored in its servers could not be fully processed because its computers were overheating and not enough electricity was available to cool them.

Faced with this sheer volume of information, often compartmentalized because of the confidentiality that weighs upon its sources and distribution, behavior unlike what is usually seen in networks tends to emerge. Hoarding "useful" information of high value becomes the norm in an environment drowning in the "noise" of databases, where the quantity of the information gathered becomes negatively correlated to its quality. The Transport Security Administration's No-Fly List is a perfect example of this unsatisfactory compromise—both in terms of security and individual freedoms. Hastily put together following the 9/11 attacks by collecting a variety of data derived from several federal agencies, the list grew from 16 individuals prevented from flying in the summer of 2001 to more than 400 names in November 2001 (Transportation Security Administration, 2002), and grew steadily thereafter to finally reach 21,000 names in 2012 (Associated Press, 2012). Another American database called the Terrorist Identities Datamart Environment (TIDE), maintained by the National Counterterrorism Center, is said to contain more than 875,000 names as of May 2013, with a 62 percent increase in the number of suspected individuals between 2009 and 2013 (Hosenball, 2013). Thus, to offset these bloated but mostly useless databases, we are witnessing the reconstruction of rather "clandestine" information-sharing interpersonal networks. They are fueled by resilient trust, but unlike their terrorist counterparts, they exist outside of decisional structures rather than as dominant organizational practices. The Canadian RCMP was notoriously chastised in the Maher Arar affair for providing its American counterpart with three CDs containing intelligence materials collected over several months of investigation, in direct violation of established information sharing procedures (Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, 2006b).

The legality paradox

The third paradox, which seems to frequently be underestimated by those in favor of organizational isomorphism, concerns the question of the legality of actions taken and the democratic oversight of anti-terrorist networks. "Dark" networks—whether they are criminal or terrorist—are particularly well adapted to their primary

role, which is to survive (avoid being arrested) and to prosper (gain ground and implement new sleeper cells respectively) in a hostile environment (Raab and Milward, 2003). As mentioned earlier, the resources the state rallies against them do not always match the agility and flexibility derived from the trust that unites their members, thus creating an asymmetrical context. The constraints for anti-terrorist networks are quite different. The obligation for results (prevent terrorist attacks and loss of life) is mixed with an obligation of means (preserve individual freedoms) defined by constitutional documents (the Canadian Charter of Rights and Freedoms and Habeas corpus for example) and implemented by the highest courts.

Even if the exceptional legislation passed for emergency purposes following 9/11 (Patriot Act in the US, Act C-36 in Canada, LSQ in France etc.) has chipped away at the foundations of our individual freedoms, such as privacy rights and limitations on arresting and detaining suspects, many legal provisions continue to guarantee citizens in Western democracies the protection of procedural safeguards on terrorism investigations. However, anti-terrorist networks can dilute these accountability mechanisms by strategically delegating tasks and responsibilities to partners subject to less stringent oversight. Thus the international network of secret prisons established by the US government delegated the most extreme interrogation and torture responsibilities to allies in the Middle East, while relying on private companies to transport prisoners captured in violation of international law. The US security and intelligence agencies that identified "targets," formulated questions to ask them, and analyzed the obtained information could not justify such a lack of accountability to the public (Hersh, 2004; Mayer, 2005). In Canada, the Arar case highlighted disclosure practices and intelligence sharing between the RCMP and US organizations. They constitute another example of tension that can arise between legality and effectiveness at the core of anti-terrorist networks, which can have potentially disastrous consequences for democratic values (Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, 2006b). These two examples clearly demonstrate to what extent mono-institutional control mechanisms have become obsolete in a security environment where subcontracting and delegating responsibilities has become commonplace. In such a context, whole-of-government or networked oversight mechanisms must be as functionally as they are institutionally focused and must consider the diversity of actors participating in each anti-terrorist program or investigation.[4]

Unlike terrorist networks' knowledge sharing approaches, which enables them to escape the need for formal bureaucratic structures, the legality paradox will expose anti-terrorism networks to an adaptation process where intelligence oversight mechanisms will gradually reflect the procedural complexity and organizational diversity of these new security assemblages.

Conclusion

The three paradoxes described in the previous paragraphs demonstrate the degree to which the new orthodoxy of the anti-terrorist fight oversimplifies important issues. In this new orthodoxy, the structure of networks could be leveraged by

government agencies just as easily as they are by clandestine groups. This is not to deny the contributions that can be offered through more flexible partnerships, better flows of information, and better understanding of the resources available within and outside of state spheres. However, the proclamation of the network as a better alternative to vertical bureaucratic structures (or the market) does not take into consideration the complexity of existing anti-terrorist systems, which operate simultaneously under these three models. As Olsen (2006) reminds us, these three morphologies have a much greater analytical potential when they are considered as complementary variables to all organizational structures, rather than being evaluated separately as ideal types that can be substituted for each other. Such an approach involves studying the optimal "degree" of centralization, hierarchical and contractual relationships, or even the flexibility with regard to objectives, resources and specific organizational contingencies. These types of evaluative studies are unfortunately too often led by inquiry commissions created in the midst of political crises following notorious failures of security services (in the case of 9/11) or the exposure of abuses of power (in Arar's situation). The fight against terrorism is such a politically charged subject that it is difficult (unlikely, a pessimist would say) to envisage such evaluations being carried out with the scientific rigor needed, precisely because the disruptive potential of such studies is too threatening for many intelligence and police agencies. However, such studies could bring us back to a reality packed with nuances and contradictions that frequently elude the trendiest theoretical models. These anti-terrorist theories, like Baudelaire's Albatross, indeed seem too often to be the kings of the conceptual sky, but prove unable to walk because of their giant wings when they are exiled on Earth.

Notes

1 This is demonstrated by the errors made concerning the lawyer Brandon Mayfield, who was wrongly arrested as a suspect in connection with the Madrid attacks on 11 March 2004; Rayed Mohammed Abdullah Ali, who was deported from New Zealand in 2006 for presumably having connections with Al-Qaeda members; or Maher Arar, who was wrongfully detained and deported by the US government to his native Syria, where he was tortured for almost a year before being declared innocent of any involvement with terrorists. Mayfield was arrested because an error occurred in the analysis of a fingerprint found on one of the bombs. His conversion to Islam, the fact that he defended an individual suspected of belonging to an Al-Qaeda cell operating out of Portland, Oregon, in a child custody case, and a phone call from his wife to an Islamic charitable organization were the determining factors in his arrest (Stout, 2006). As for Ali, his untimely circumstances were that he was a Saudi who had taken courses in the same pilot training school as one of the 9/11 terrorists and briefly shared an apartment with that same individual. His name's presence on a diagram put online by a network analysis consultant showing his close proximity to the 9/11 terrorist considerably increased the suspicions of the New Zealand authorities responsible for his file (Cumming, 2006).
2 For a detailed timeline, see the Electronic Frontier Foundation website at www.eff.org/nsa-spying/timeline, last accessed on 8 August 2014.
3 Other estimates are much lower, although still impressive at a couple of exabytes of storage (Jennings, 2013).

4 See the recommendations of the O'Connor Commission concerning the control mechanisms of the RCMP and the other federal agencies acting in the national security sector (Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, 2006a).

References

9/11 Commission (National Commission on Terrorist Attacks upon the United States) (2004) *Final Report*. New York: W. W. Norton and Company.

Ackerman, S. (2013) NSA violations led judge to consider viability of surveillance program. *Guardian*. 10 September.

Amicelle, A. (2011) Towards a "new" political anatomy of financial surveillance. *Security Dialogue*. 42 (2), pp. 161–178.

Arkin, W. (2002) Military strategy—mapping the minds in Iraq's regime: social scientists take aim at Saddam Hussein. *Los Angeles Times*. 1 September.

Arquilla, J. and Ronfeldt, D. (2001) The advent of netwar (revisited). In Arquilla, J. and Ronfeldt, D. (eds) *Networks and Netwars*. Santa Monica CA: Rand.

Associated Press (2012) US "no-fly" list of suspected terrorists doubles in 12 months. *Guardian*. 2 February.

Bamford, J. (2012) The NSA is building the country's biggest spy center (watch what you say). *Wired*. 15 March. Available at: www.wired.com/threatlevel/2012/03/ff_nsadata-center/. Accessed 27 November 2013.

Benkler, Y. (ed.) (2006) *The Wealth of Networks*. New Haven: Yale University Press.

Braithwaite, J. (2000) The new regulatory state and the transformation of criminology. *British Journal of Criminology*. 40 (2), pp. 222–238.

Brodeur, J.-P. (ed.) (2010) *The Policing Web*. Oxford: Oxford University Press.

Brodeur, J.-P. and Dupont, B. (2006) Knowledge workers or "knowledge" workers? *Policing and Society*. 16 (1), pp. 7–26.

Burkeman, O. and Tuckman, J. (2003) Firm in Florida election fiasco earns millions from files on foreigners. *Guardian*. 5 May.

Canadian Security Intelligence Service (2013) *The Future of Al-Qaeda: Results of a Foresight Project*. Ottawa: CSIS.

Carley, K., Lee, J.-S. and Krackhardt, D. (2002) Destabilizing networks. *Connections*. 24 (3), pp. 79–92.

Castells, M. (ed.) (2000) *The Rise of the Network Society: The Information Age—Economy, Society and Culture*. 2nd edn. Oxford: Wiley.

Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar (2006a) *A New Review Mechanism for the RCMP's National Security Activities*. Ottawa: Government of Canada.

Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar (2006b) *Report of the Events Relating to Maher Arar: Analysis and Recommendations*. Ottawa: Government of Canada.

Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182 (2010) *Final Report—Volume 2: Pre-Bombing, post-Bombing Investigation and Response*. Ottawa: Government of Canada.

Cumming, G. (2006) Saudi student pilot in the wrong place at the wrong time. *New Zealand Herald*. 5 August.

Deflem, M. (ed.) (2002) *Policing World Society: Historical Foundations of International Police Cooperation*. New York: Oxford University Press.

Deibert, R. J. and Stein, J. G. (2002) Hacking networks of terror. *Dialogue IO*. 1 (1), pp. 1–14.

Dizard, W. (2005) NSA searches for novel intel answers in the Glass Box. *GCN*. 17 June. Available at: http://gcn.com/Articles/2005/06/17/NSA-searches-for-novel-intel-answers-in-the-Glass-Box.aspx. Accessed 27 November 2013.

Dupont, B. and Pérez, E. (eds) (2006) *Les Polices au Québec*. Paris: Presses Universitaires de France.

Finnegan, W. (2005) The terrorism beat: How is the NYPD defending the city? *The New Yorker*. 81 (21), pp. 58–71.

Friel, B. (2002) Hierarchies and networks. *Government Executive*. 1 April. Available at: www.govexec.com/features/0402/0402s2.htm. Accessed 9 August 2014.

Gagnon, C. and Bacher, J.-L. (2004) Le dispositif canadien de lutte contre le blanchiment d'argent. *Revue Internationale de Criminologie et de Police.* 57, pp. 428–437.

Garreau, J. (2001) Disconnect the dots. *Washington Post*. 17 September, p. C1.

Gorman, S. (2007) Budget falling short at NSA. *Baltimore Sun*. 17 January. Available at: http://articles.baltimoresun.com/2007-01-17/news/0701170100_1_alexander-budget-spy-agency. Accessed 9 August 2014.

Government Accountability Office (2006) *Critical Infrastructure Protection: Progress Coordinating Government and Private Sector Efforts Varies by Sectors' Characteristics*. Washington DC: Government Accountability Office.

Granovetter, M. (1973) The strength of weak ties. *The American Journal of Sociology*. 78 (6), pp. 1360–1380.

Gunaratna, R. (2004) Le nouveau visage d'Al Qaida: La menace du terrorisme islamiste après le 11 septembre. In Chaliand, G. and Blin, A. (eds) *Histoire du terrorisme de l'antiquité à Al-Qaïda*. Paris: Bayard, pp. 463–483.

Hersh, S. (ed.) (2004) *Chain of Command*. New York: Harper Collins.

Hobbs, R. (ed.) (2003) *Mark Lombardi: Global Networks*. New York: Independent Curators International.

Hoffman, B. (ed.) (2006) *Inside Terrorism*. New York: Columbia University Press.

Hosenball, M. (2013) Number of names on U.S. counter-terrorism database jumps. Reuters. 2 May. Available at: www.reuters.com/article/2013/05/03/us-usa-security-database-idUSBRE94200720130503. Accessed 27 November 2013.

Innes, M. (2006) Policing uncertainty: Countering terror through community intelligence and democratic policing. *The Annals of the American Academy of Political and Social Science*. 605 (1), pp. 222–241.

Jennings, R. (2013) NSA's huge Utah datacenter: How much data will it store? Experts disagree. *Forbes.com*. 26 July. Available at: www.forbes.com/sites/netapp/2013/07/26/nsa-utah-datacenter/. Accessed 27 November 2013.

Johnston, D. and Jehl, D. (2005) FBI's recruiting of spies causes new rift with CIA. *New York Times*. 11 February. Available at: www.nytimes.com/2005/02/11/politics/11intel.html?_r=0. Accessed 9 August 2014.

Jurgensmeyer, M. (2000) Understanding the new terrorism. *Current History*. 99 (636), pp. 158–163.

Kadzik, P. (2013) *2012 Annual report on FISA implementation*. U.S. Department of Justice, Washington DC.

Klerks, P. (2001) The network paradigm applied to criminal organizations: Theoretical nitpicking or a relevant doctrine for investigators? Recent developments in the Netherlands. *Connections*. 24 (3), pp. 53–65.

Knoke, D. (2013) "It takes a network": The rise and fall of social network analysis in U.S. Army counterinsurgency doctrine. *Connections*. 33 (1), pp. 1–10.

Labi, N. (2006) Jihad 2.0. *The Atlantic Monthly*. 297 (6), pp. 102–108.

Laqueur, W. (1999) *The New Terrorism: Fanaticism and the Arms of Mass Destruction*. Oxford: Oxford University Press.

Law Enforcement News (2005) Critical mass builds among chiefs for real-time terrorism info network. *Law Enforcement News*. 31 (636), p. 6.

Lesser, I., Hoffman, B., Arquilla, J., Ronfeldt, D., Zanini, M. and Jenkins, B. (eds) (1999) *Countering the New Terrorism*. Santa Monica CA: Rand Corporation.

Lewis, J. (2013) *Al-Qaeda in Iraq Resurgent*. Washington: Institute for the Study of War.

Lichtblau, E. (2004) Homeland Security Department experiments with new tool to track financial crime. *New York Times*. 12 December. Available at: www.nytimes.com/2004/12/12/politics/12finance.html. Accessed 9 August 2014.

Lichtblau, E. and Mazzetti, M. (2007) Military expands intelligence role in U.S. *New York Times*. 14 January. Available at: www.nytimes.com/2007/01/14/washington/14spy.html?pagewanted=all. Accessed 9 August 2014.

Lowndes, V. and Skelcher, C. (1998) The dynamics of multi-organizational partnerships: An analysis of changing modes of governance. *Public Administration*. 76 (2), pp. 313–333.

Luhmann, N. (ed.) (1979) *Trust and Power*. Chichester: Wiley.

Markle Foundation Task Force (2003) *Creating a Trusted Information Network for Homeland Security*. Washington DC: Markle Foundation.

Mayer, J. (2005) Outsourcing torture. *The New Yorker*. 14 February, pp. 106–123.

McChrystal, S. (2011) It takes a network. *Foreign Policy*. March–April, pp. 6–9.

Monahan, T. and Palmer, N. (2009) The emerging politics of DHS fusion centers. *Security Dialogue*. 40 (6), pp. 617–636.

Morabito, A. and Greenberg, S. (2005) *Engaging the Private Sector to Promote Homeland Security: Law Enforcement – Private Security Partnerships*. Washington DC: U.S. Department of Justice.

Morselli, C. (2007) The efficiency/security trade-off in criminal networks. *Social Networks*. 29 (1), pp. 143–153.

Mueller, R. (2006) Citizens Crime Commission James Fox Memorial Lecture. 26 April. Available at: www.fbi.gov/news/speeches/unity-the-greatest-weapon-against-terrorism. Accessed 9 August 2014.

Murphy, V. (2001) Spook Valley. *Forbes Magazine*. 12 October, pp. 12–16.

Nadelmann, E. (1997) *Cops across Borders: The Internationalization of US Criminal Law Enforcement*. University Park: Pennsylvania State University Press.

Nakashima, E. (2007) The legal tangles of data collection. *The Washington Post*. 16 January.

Office of the Inspector General (2004) *The Federal Bureau of Investigation's Foreign Language Program—Translation of Counterterrorism and Counterintelligence Foreign Language Material*. Washington DC: Department of Justice.

Olsen, JP. (2006) Maybe it is time to rediscover bureaucracy. *Journal of Public Administration Research and Theory*. 16 (1), pp. 1–24.

Pincus, W. (2005) Pentagon will review database on US citizens. *Washington Post*. 15 December.

Priest, D. and Arkin, W. (2010) A hidden world, growing beyond control. *Washington Post*. July 19, pp. A1 and A6–A9.

Raab, J. and Milward, H. B. (2003) Dark networks as problems. *Journal of Public Administration Research and Theory*. 13 (4), pp. 413–439.

Rhodes, R. (2006) The sour laws of network governance. In Fleming, J. and Wood, J. (eds) *Fighting Crime Together: The Challenges of Policing and Security Networks*. Sydney: University of New South Wales Press.

Ring, P. S. (1996) Fragile and resilient trust and their roles in economic exchange. *Business and Society*. 35 (2), pp. 148–175.

Risen, J. and Lichtblau, E. (2005) Bush lets US spy on callers without courts. *New York Times*. 16 December.

Sheptycki, J. (2004) Organisational pathologies in police intelligence systems. *European Journal of Criminology*. 1 (3), pp. 307–332.

Shorrock, T. (ed.) (2008) *Spies for Hire: The Secret World of Intelligence Outsourcing*. New York: Simon and Schuster.

Spalek, B. (2010) Community policing, trust, and Muslim communities in relation to "new terrorism." *Politics and Policy*. 38 (4), pp. 789–815.

Spalek, B. and Lambert, R. (2008) Muslim communities, counter-terrorism and counter-radicalisation: A critically reflective approach to engagement. *International Journal of Law, Crime and Justice*. 36 (4), pp. 257–270.

Stout, D. (2006) Inquiry says FBI erred in implicating man in attack. *New York Times*. 6 January.

Taylor, R. and Russell, A. (2012) The failure of police "fusion" centers and the concept of a national intelligence sharing plan. *Police Practice and Research*. 13 (2), pp. 184–200.

Thatcher, D. (2005) The local role in homeland security. *Law and Society Review*. 39 (3), pp. 635–676.

Tilly, C. (ed.) (2005) *Trust and Rule*. Cambridge: Cambridge University Press.

Transportation Security Administration (2002) *TSA Watch Lists*. Washington DC: Transportation Security Administration. Powerpoint presentation obtained by the ACLU of Northern California. Available at: www.aclunc.org/sites/default/files/asset_upload_file371_3549.pdf. Accessed 27 November 2013.

Tufte, E. R. (ed.) (1990) *Envisioning Information*. Cheshire CT: Graphics Press.

Van Meter, K. M. (2002) Terrorists/liberators: Researching and dealing with adversary social networks. *Connections*. 24 (3), pp. 66–78.

Weimann, G. (ed.) (2006) *Terror on the Internet: The New Arena, The New Challenges*. Washington DC: United States Institute of Peace.

Xu, J. and Chen, H. (2005) CrimeNet explorer: A framework for criminal network knowledge discovery. *ACM Transactions on Information Systems*. 23 (2), pp. 201–226.

10 The promise and perils of integrated models of public safety in Canada

Veronica M. Kitchen and Adam Molnar

Introduction

In 2011, Canada's Ministry of Public Safety released Canada's first counter-terrorism strategy, "Building Resilience Against Terrorism." In keeping with similar documents released by its allies, Canada's strategy stresses a holistic approach to counter-terrorism policy that "sets out Canada's integrated approach to dealing with terrorist threats, both at home and abroad … [which] … explains how Canada's local, national, and international efforts support each other to protect Canadians and Canadian interests" (Department of Public Safety, 2013, p. 6). While the primary *aim* of the strategy is "to counter domestic and international terrorism in order to protect Canada, Canadians and Canadian interests," the primary *means* to achieve the aim are through enhanced partnerships, which "are central to the success of the Strategy" (Department of Public Safety, 2013, p. 6).

The key underlying assumption of the document is that increased partnerships will provide a galvanized response to potential terrorist threats. Achieving the goals laid out in the document depends on an integrated approach that reaches across "all levels of government, law enforcement agencies, the private sector and citizens, in collaboration with international partners and key allies, such as the United States" (Department of Public Safety, 2013, pp. 4, 6). While security integration is not a new phenomenon in Canadian security policy, after 9/11 the modus operandi of integration was unabated as a panacea to potential terrorist threats. The practice of integrating institutions is not unique to Canada and can be widely noted in similar counter-terrorism strategies among Canada's allies. While integration in Canada no doubt has some unique aspects, such as the close but asymmetrical relationship with the United States, the conclusions we draw here are likely to be broadly applicable in other cases.

Pre-9/11 lessons about integration were reinforced in the popular and policy imagination after the 9/11 terrorist attacks. As shown by the American 9/11 Commission Report and similar reports, policy-makers have gravitated toward the idea that stopping terrorism is as much a problem of connecting pieces of information already in the possession of authorities as it is a problem of gathering new information. Like its allies, Canada identified the need for interagency cooperation in strategic documents and reports issued after the terrorist attacks,

and ushered in institutional change driven by a move toward integration. Canada's first security strategy written after 9/11, *Securing an Open Society* (Privy Council Office, Government of Canada, 2004), argues that

> The Government is building a fully integrated security system that ensures that we can more effectively respond to existing threats and quickly adapt to new ones. The evolving nature of threats to Canadians requires a fully integrated government approach that ensures that issues and information do not fall between the different parts of our security system. This system needs to be fully connected to key partners—provinces, territories, communities, first line responders, the private sector and Canadians.
>
> (Privy Council Office, 2004)

Collaboration and partnerships in national security existed well before the release of *Securing an Open Society* or *Building Resilience Against Terrorism.* What is new, however, is that since 9/11 integration has become a more explicit and taken-for-granted discourse—and as such, it has faced little scrutiny as an object of study, and there are few scholarly appraisals of its worth as an emerging policy instrument. It is not uncommon to hear that greater integration will inherently yield more efficient or effective results in counter-terrorism policy (Canadian Association of Chiefs of Police, 2007, 2004; Department of Public Safety, 2013). However, much of this discourse exists in the complete absence of evidence-based evaluative research. The trend toward integration is still largely based more on actuarial assumptions and less on independent empirical research and analysis that considers the advantages and disadvantages of enhanced integrated approaches to law enforcement and national security. Our chapter maps the current trends of integration in Canadian counter-terrorism policy with the goal of identifying instances where integration has clear benefits and those where the advantages are less clear or otherwise problematic. Using Canada as a case of a broader phenomenon, we map how integration is unfolding in the areas of intelligence-led policing, partnerships in the monitoring and detection of activities of individuals who are suspected of posing a terrorist threat, collaboration in the deterrence or disruption of capabilities of individuals who are suspected of carrying out terrorist activities, and integration within emergency management in disaster response scenarios.

The integrated model of security we discuss here comprises both the integration of the technical architecture that shapes the information and data sharing protocols across databases, and the integration of organizations, people, and the legal and policy environments through which they operate. The integrated model of national security, then, attempts to integrate the many technical and social facets of institutions and people across federal, provincial and municipal agencies, but also across different parts of the security bureaucracy, between different law enforcement, military and intelligence agencies. In many cases, integrated networks and institutions have also reached beyond federal, provincial and municipal governments and into communities, the private sector, and with foreign partners, with serious technical, legal and social implications.

This chapter draws on government documents, newspaper reports and other publicly available sources. The authors have each also completed a series of interviews with policy-makers and operations officials working with or in integrated national security and policing institutions in Canada, at various levels of government, over the past six years.

Integration in Canadian counter-terrorism strategy

Building Resilience Against Terrorism (hereafter counter-terrorism or CT strategy) "sets out Canada's integrated approach to dealing with terrorist threats, both at home and abroad" through "all levels of government, law enforcement agencies, the private sector and citizens, in collaboration with international partners and key allies, such as the United States" (Department of Public Safety, 2013, p. 6). The strategy brings together into one document a series of policies and strategies that had been evolving since 9/11 (and in some cases before). The government understands the evolving terrorist threat to be increasingly "decentralized and diverse," and the strategy attempts to respond with an "adaptable and forward-looking" approach (Department of Public Safety, 2013, p. 6). Put another way, the CT strategy falls in line with trends after 9/11 that denote a wider shift towards *preventive* models of counter-terrorism and crime (Zedner, 2009). In order to forestall or disrupt the potential for a terrorist attack or violence, the strategy insists that "cooperation and seamless information sharing within and between security intelligence agencies and law enforcement is essential to effectively address the terrorist *threat*" (Department of Public Safety, 2013, p. 11).[1] This shift to prevention or pre-emption may be inherent in social constructions of terrorism as a threat that is difficult to predict due to its low probability. Aradau and van Munster argue that as governments try to predict the future, they tend to focus on worst-case scenarios and shift the burden of proof to citizens to prove that they are not terrorist risks (Aradau and van Munster, 2007). Under conditions of uncertainty—where we cannot know what a terrorist attack will look like, when it will come, or who will perpetrate it—this has the effect of making surveillance and control mechanisms that act on the whole population more desirable (Aradau and van Munster, 2007). Given the limits of intelligence and surveillance tools, a decision about who (or what) is a threat becomes an administrative decision based on the goal of maintaining zero risk, rather than a decision based on careful weighing of the evidence (Aradau and van Munster, 2007). In addition, security officials are often implicated in a form of "reputational risk," where the negative prospect that a terrorist attack occurs under the jurisdictional authority of an official will incentivize an enhanced intelligence-led surveillance strategy.

The government partnerships identified in the CT strategy blur the traditional boundaries between domestic national security policy and foreign and defense policy; reaching across international, federal, provincial and municipal agencies as well as community groups and individuals. For instance, Canadian agencies have a particularly close relationship with the United States, and in some cases collaborate in transnationally integrated institutions such as the

Integrated Border Enforcement Teams (IBETs) and the Integrated Cross-Border Maritime Law Enforcement Operations, better known as Shiprider. The CT strategy insists on close collaboration with allies, established international organizations such as the North Atlantic Treaty Organization (NATO), and other groups such as the G8 and the Global Counter-terrorism Forum. Since 9/11, a driving feature of counter-terrorism policy has been an insistence on intelligence-led approaches to stem, deter or disrupt the potential for terrorist attack. As a result, Canada's global signals intelligence (SIGINT) partnerships have been turned more and more toward counter-terrorism activities, including increased assistance to law enforcement. These law enforcement and intelligence sharing partnerships reach across a range of federal, provincial and municipal networks and are central to the official counter-terrorism response in Canada. The CT strategy also insists on government partnerships with the private sector, non-governmental organizations (NGOs) "to protect the nation's critical infrastructure and bolster the resilience of communities," and citizens to "provide the most effective avenue to strengthen society as to maximize resistance to violent extremism" (Government of Canada, Department of Public Safety, 2013).

In the context of these partnerships, the CT strategy emphasizes four mutually reinforcing pillars to Canada's counter-terrorism policy in order to

- *prevent* individuals from engaging in terrorism;
- *detect* the activities of individuals and organizations who may pose a terrorist threat;
- *deny* terrorists the means and opportunity to carry out their activities; and
- *respond* proportionately, rapidly, and in an organized manner to terrorist activities and mitigate their effects (Department of Public Safety, 2013).

Across these dimensions, counter-terrorism policy in Canada entails a broad and heterogeneous field of actors, strategies, tactics and distinct responsibilities. By extension, integration, while existing as a common trend in joined-up government approaches to counter-terrorism, emerges in complex and contradictory ways in Canada's counter-terrorism framework. Public safety governance, and counter-terrorism policy more generally, is by no means a seamless and unified project. To fully comprehend the extent to which integration has become an animating feature of counter-terrorism policy that hybridizes national security, law enforcement, private sector activities and citizenship, the following section of the chapter discusses how integration is unfolding in each of the four main areas within Canada's counter-terrorism strategy. The policies discussed in these categories blur into one another, and our use of them should therefore be viewed as an organizational tool rather than as a reflection of stark differences between them.

Prevent: monitoring and intervening in radicalization

The first element of the CT strategy focuses on the motivations of individuals who are suspected of engaging in or "who have the potential to engage in

terrorist activities at home or abroad" (Department of Public Safety, 2013, pp. 11–12). Threats from such individuals are understood by Public Safety to emerge through a process of "radicalization," which is a usually a prerequisite to acts of violent extremism. Radicalization is understood in the CT strategy as "a process by which individuals are introduced to an overtly ideological message and belief system that encourages movement from moderate, mainstream beliefs towards extremist views." The threat to national security emerges when radicalization leads to "violence as a means of promoting political, ideological, or religious objectives" (Department of Public Safety, 2013, p. 12). Preventing such radicalization, and being able to determine when a radicalized individual is likely to turn violent, is a key component in the prevent strategy.[2]

Integration in "prevent initiatives" entails extensive partnerships between government authorities, communities and citizens. Partnerships are exemplified through the Cross-Cultural Roundtable on Security (CCRS), which is a joint-project between Public Safety and the Department of Justice, as well as the RCMP's National Security Community Outreach (NSCO) program, which focuses directly on "the threat of radicalization leading to violent extremism through local initiatives" that seek to address and indemnify "the concerns of minority communities" (Department of Public Safety, 2013, p. 14). These initiatives are intended to foster a culture of trust and communication between authorities and citizens, and the RCMP and CSIS are focusing on developing their capabilities and associations with police forces in other domestic jurisdictions and community groups as a way to stem the potential for terrorism. Through such partnerships, Public Safety authorities provide "alternative narratives that emphasize the open, diverse and inclusive nature of Canadian society and seek to foster a greater sense of Canadian identity and belonging for all" (Department of Public Safety, 2013, p. 15). Domestically, these partnerships include liaising with citizen groups on a regular basis and can often have the effect of inciting distrust in the communities where the tactic is used (Apuzzo and Goldstein, 2014; Thacher, 2005; Office of the Privacy Commissioner of Canada, 2009). In international terms, Public Safety Canada is collaborating across a range of agencies, including the Department of Foreign Affairs, Trade, and Development (DFATD), RCMP, Canadian Security Intelligence Services, the Department of National Defence and the Canadian Forces (DND/CF) and the Canadian International Development Agency (CIDA). The purpose of these partnerships is to facilitate more efficient operations, to identify and address the perceived causes of terrorism, and to present a favorable image of Canada abroad.

Detect: security intelligence integration

The second purpose of the CT strategy is to "detect the activities of individuals and organizations who may pose a terrorist threat" (Department of Public Safety, 2013, p. 15). Countering potential threats entails knowledge of "the terrorists themselves, their capabilities and the nature of their plans" (Department of Public Safety, 2013, p. 15). Most significantly, the detect strategy relies on

enhanced intelligence capacity and capabilities, understanding the nature of the threat environment, and "extensive collaboration and information sharing with domestic and international partners" (Department of Public Safety, 2013, p. 15). Such integration relies heavily on national security intelligence, which is defined as "a process that includes coercive or covert acquisition of data about security issues, events and responses" (Lippert and O'Connor, 2006, p. 53) and requires strong capabilities for the collection, analysis, and distribution of usable or actionable intelligence. In Canada, such surveillance and information sharing has led to the blurring of the distinction between terrorism and political protest under the category "multi-issue extremism" (Monaghan and Walby, 2012). It is considered a key component in disrupting and detaining persons who are perceived to present risks of terrorism or who are otherwise suspected of "radicalization" and may exhibit a potential to damage property or urban infrastructure (see, for instance, CSIS's public report where multi-issue extremism is categorized as terrorism: Government of Canada, CSIS, 2014).

The primary agencies collecting and sharing intelligence in Canada include CSIS, the Communication Security Establishment Canada (CSE) and the RCMP. The RCMP and CSIS use a full range of collection methods that include (among others) human intelligence through infiltration (HUMINT), surveillance, and open-source intelligence (OSINT) tactics such as information collection through online sources including social media (Canadian Access to Social Media Information (CATSMI) Project, 2013). Another significant source of intelligence collection rests with CSE that provides foreign signals intelligence (SIGINT) as well as other "technical and operational support to law enforcement and security intelligence agencies" (Department of Public Safety, 2013, p. 16). CSE, in particular, offers assistance to lawful access across a wide range of government agencies under their "Mandate C," including a non-exclusive list of:

> The RCMP and CSIS, and, second, the other federal government departments and agencies with law and regulatory enforcement functions, including the Canada Border Services Agency, Canada Revenue Agency, Citizenship and Immigration Canada, Health Canada, Environment Canada, Industry Canada, Transport Canada, the Canadian Food Inspection Agency, the Department of Fisheries and Oceans.
>
> (Communication Security Establishment Canada, 2007)

Collection also occurs at the border with population, material objects and currency flows, with the Canadian Border Services Agency (CBSA), through the Department of Finance with information exchange between FINTRAC and other "terrorist-financing" response initiatives, as well as with other foreign-based agencies such as the DND/CF and DFAIT who marshal their overseas capabilities.

Interestingly, global intelligence partnerships are not explicitly mentioned in the CT strategy, in spite of their significant place in Canada's integrated approach to preventing terrorist attack. The globally integrated intelligence

partnership comprises of the "Five Eyes" alliance of states, which includes cognate agencies from the United States, the United Kingdom, Canada, Australia and New Zealand. These partners rely on modern global communication information systems for conducting cross-border surveillance and information sharing among the parties. Of late, Five Eyes intelligence collection and sharing has been increasingly controversial and has been found by national governments such as Germany and Brazil, by major private sector IT organizations such as Google and Apple, and by civil advocacy organizations around the world to be operating in contravention to currently existing legal, normative and human rights standards (Freeze, 2013; Privacy International, 2013; Kehl, 2014). Integration, then, has not been universally seen to be a public good.

Other international partnerships include the globally orchestrated Financial Action Task Force (FATF), which monitors global financial flows with the intention to disrupt money laundering and terrorist financing initiatives. Enhanced cooperation and information exchange on financial matters are also facilitated through the Egmont Group, which is a global forum dedicated to facilitating the sharing of information expertise among financial intelligence units around the world.

The domestic security intelligence network was faced with a valuable opportunity to further refine its capabilities during the Vancouver 2010 Winter Olympics and the G8/20 political summit. The RCMP-ISU sat atop the security-intelligence chain of command in the lead-up to the Olympics. While early stages of intelligence gathering were conducted under a newly conceived Joint-Intelligence Group (ISU-JIG), which was formed in 2005, the security intelligence apparatus underwent further change during this period. The ISU-JIG was initiated by the RCMP and consisted of partners from municipal and provincial police forces, Canadian Forces and CSIS. In 2007, the ISU-JIG issued a report that cited its primary responsibility to "develop a comprehensive public-order portfolio to monitor and assess high risk groups, individuals, and potential threats to Olympic-related events" (ISU-JIG, 1 April 2007). The JIG continued as a central organization in collecting intelligence in conjunction with the CSIS-led Integrated Threat Assessment Centre (ITAC) (which was established in 2004, and which subsequently changed its name to the Integrated Terrorism Assessment Centre in 2012).

Intelligence operations for counter-terrorism investigations and public-order policing at the Vancouver 2010 Olympics were centralized under the JIG-ISU. Strategic intelligence reports were communicated as daily intelligence reports to municipal law enforcement officials (Molnar, 2013). Further, as many as half of the JIG members were Vancouver municipal police, illustrating the extent to which integration in national security and law enforcement is also increasingly reaching across federal and municipal governance networks (Molnar, 2013).

The vastness of the integrated nature of intelligence sharing in the area of counter-terrorism, spurred ahead through Olympic-related preparations, is represented in an email written in October 2006 by RCMP Director General of National Security, Al Nause. According to Mr. Nause:

> ITAC is comprised of several persons from different constituting agencies including the RCMP, CSIS, FAC, TC, Health Canada, CSC, and CBSA, etc.… Each person, in our case the RCMP member on secondment, has access to their respective agency data banks; e.g., SPROS, SCIS et.… Because ITAC has the expertise and the access to a wealth of information interdepartmentally and abroad, the RCMP as well as many other departments rely on ITAC to provide strategic threat assessments.
>
> (Al Nause, email, 24 October 2006, cited in Monaghan and Walby, 2012)

Integration in the area of security intelligence, a primary tool in intelligence-led approaches to counter-terrorism, is not only trending toward the integration of more traditional intelligence, security and law enforcement agencies but is also expanding in scope to include officials situated in organizations with mandates that are not traditionally associated with security operations. For instance, the security intelligence apparatus of ITAC draws on access to Transport Canada, Health Canada, Correctional Services Canada and other international partners to develop strategic threat assessments.

Given the wealth of information that is available to ITAC by drawing from a range of security and non-security agencies across federal, provincial and municipal agencies, ITAC intelligence reports are vital for categorizing, framing and prioritizing national security concerns in Canada (Monaghan and Walby, 2012). And, notably, such risk profiles regularly filter down to the municipal level on a daily basis. If we look beyond ITAC and into the realm of signals intelligence, further points of cooperation remain. The extent to which CSE collaborates with CSIS, the RCMP, the Department of National Defence, and Canadian Border Services through "Support to Lawful Access" requests is still murky, but documents recently released under the Access to Information act suggest that requests for CSE support to other Canadian security organizations number between 70 and 80 a year (Freeze, 2013). While CSE provides support only after the relevant domestic agencies acquire a warrant to receive CSE assistance, questions remain regarding the lawfulness of how such warrants are crafted and acted upon. In particular, a recent ruling by Justice Mosley, a key architect of Canada's anti-terrorism legislation, found that CSIS had inappropriately requested the assistance of CSE while also hiding from the court that CSE also requests assistance from its partners to monitor Canadians travelling abroad (Federal Court, 2013). Mosley argued that by circumventing legal requirements that regulate integration, CSIS's and CSE's actions can endanger the Canadians being monitored. While there is a lack of long-term data concerning CSE's assistance to domestic agencies, the legality of such assistance is now being questioned in federal courts.

The domestic realm of intelligence involves a different articulation. CSIS is the primary organization for domestic intelligence and has been expanding the scope of its network in recent years. A domestic structural sedimentation of an evolving intelligence capability is characterized through a preemptive approach to risk management and security threat assessments in Canada. An increase in

the scope of partners affiliated with the Integrated Terrorist Threat Assessment Centre (ITAC) has grown to include a wide range of actors and agencies. The number of partners now included in ITACs policy network include the RCMP, CSIS, FAC, TC, CSC, Health Canada and the CBSA, to name only a few. The range of actors now linked together are further fused by actors that are seconded to ITAC, which means these members are able to "link" ITAC with their respective partners' informational databanks without traditional oversight mechanisms that might require judicial authorizations. For instance, the Secure Police Reporting and Occurrance System (SPROS) database,[3] under the auspices of the RCMP, can now be tied into the expertise and wealth of information that ITAC (and other partners in the nexus) can acquire both interdepartmentally and abroad. Under these new normative, ideational and structural conditions, ITAC becomes a primary authority for categorizing, framing and triaging national security risks, which, as we will see, can lead to problems in the accuracy, coherence and implementation of the threat categorization being developed as they move across jurisdictions.

The rules under which CSIS and the RCMP, in particular, share security intelligence were profoundly influenced by the conclusions of the O'Connor Commission, which investigated Canadian complicity in Maher Arar's rendition to Syria. The O'Connor Commission concluded that information sharing protocols between CSIS and the RCMP, and between Canada and the United States, were problematic. One of the outcomes of Commission was a new Memorandum of Understanding between CSIS and the RCMP which governed, among other things, information sharing between them. Standards for gathering and using information are different for the RCMP and CSIS; to gather intelligence, CSIS must only have reasonable grounds to suspect a threat to Canadian security,[4] whereas to launch an investigation the RCMP must prove that there is probable grounds to believe that a specific crime has been committed or will be committed. In either case, information sharing is centralized through RCMP and CSIS headquarters. The process of information sharing with the RCMP's foreign partners has been similarly centralized. While intelligence sharing between the RCMP and international partners used to happen mostly through liaison officers posted to embassies abroad, according to procedure it ought now to happen through headquarters, where information is evaluated and has caveats attached before sharing (Anonymous, 2013, interview, 28 October). While integration has clearly broadened the networks of integration to include more actors, it has also had the effect of centralizing intelligence collection and analysis functions through ITAC and the RCMP/CSIS Strategic Dialogue process.

In sum, intelligence at the international and domestic levels is characterized by integration in human partnerships which authorize the expansion of joint-database networks and increasing degrees of information sharing. These networks are further enhanced with a range of agencies that have not traditionally been subject to an explicit "security-oriented" mandate, with a wider proportion of potentially relevant (and usable) data points being integrated into national security intelligence collection and strategic analyses. As we will discuss near

the end of the chapter, while the inherent value of these partnerships are assumed by authorities, a full account of the implications of these enhanced partnerships may yield mixed outcomes.

Deny: Integrated National Security Enforcement Teams and Integrated Border Enforcement Teams

The third pillar of Canada's counter-terrorism strategy seeks to enhance national security capabilities to "deny terrorists the means and opportunity to carry out their activities in order to protect Canadians and Canadian interests" (Department of Public Safety, 2013, p. 18). In the "deny" initiative, integration is again regarded as key to

> deny[ing] terrorists the means and opportunities to pursue terrorist activities … [by] mitigating vulnerabilities and aggressively intervening in terrorist planning, including prosecuting individuals involved in terrorist related criminal activities, and making Canada and Canadian interests a more difficult target for would-be terrorists.
>
> (Department of Public Safety, 2013, p. 4)

While the deny initiative finds overlap with intelligence collection, analysis and sharing, it also focuses more directly on the criminal investigation of terrorist offences. Canada's Integrated National Security Enforcement Teams (INSETs) are seen as the key institution for carrying out the law enforcement functions of the "deny" objective (Government of Canada, Department of Public Safety, 2013). The INSETs are led by the RCMP and consist of members from CSIS, CBSA and provincial and municipal police forces. To date there are five such teams located across the country, in Vancouver, Edmonton, Toronto, Ottawa and Montreal. The Integrated National Security Enforcement Teams were created shortly after 11 September, emerging from the National Security Investigations Sections (NSISs) units which took over the national security and intelligence capacity of the RCMP after CSIS was severed from the force. INSETs were first mentioned in the media only a month after 9/11 (Steinbachs, 2001) and were formally launched in June of 2002 (Woods, 2002). The INSETs have a mandate to collect and analyze national security intelligence and share it with their partners, to respond to threats to national security, and to support their partners' ability to respond to national security threats (Government of Canada, Royal Canadian Mounted Police, 2013b).

Three relevant shifts characterize the emergence of the INSETs and the processes of integration in denial strategies. While the NSISs worked with local police of jurisdiction and with local CSIS officials on a case-by-case basis, this cooperation was mostly informal. Its effectiveness relied strongly on personal relationships and, quite practically, knowing who to call at the right moment (Anonymous 2013, interview, 28 October). The INSETs, by contrast, are much more formalized. They are based on memoranda of understanding and

agreements in a legalistic relationship. The second shift is a consequence of formalization. The INSETs were developed on a model that *colocated* partners from across the security bureaucracy in the same institution. This allows cooperation to happen more organically, possibly with less disruption due to changes in personnel. Finally, integration has happened simultaneously with an increase in the number of personnel involved in national security policing. While a rise in the number of security practitioners is not itself a phenomenon of integration, it does mean that a growing number of security professionals are working in integrated teams, not least to acknowledge the personal and professional contacts that travel into new institutional arrangements.

Canada uses additional integrated teams in support of its national security. Two other examples, the Integrated Border Enforcement Teams (IBETs) and Shiprider, further extend the integrated model by integrating Canadian security officials with those in the United States. The IBETs are designed to "identif[y], investigat[e] and interdict[] persons, organizations and goods that threaten the national security of one or both countries or that are involved in organized criminal activity" (Government of Canada, RCMP, 2014a). They operate at Canadian points of entry and comprise individuals from the RCMP, Canadian Border Services, and American representatives from Customs and Border Protection, Immigration and Customs Enforcement and the US Coast Guard. The perceived success of the IBETs as an integrated model of national security law enforcement at the border spawned Shiprider, an integrated program in which American Coast Guard Officials and Canadian RCMP officers share vessels and patrol Canadian waterways. After a few successful pilot programs, not least of which were tests during Superbowl XL in 2006 and the Vancouver Olympics and the Toronto G20 in 2010, the program was regularized in 2013, with two full-time teams now in operation and two more beginning in 2015 (Government of Canada, RCMP, 2013a). IBETs and Shiprider are also supposed to serve as a model for even further cross-border integration, in the form of NxtGen policing teams. The vision for the NxtGen policing teams, outlined in the Canada–United States Beyond the Border agreement, was for integrated, land-based teams to patrol between points of entry (Cross-Border Crime Forum, 2011). Discussions on NxtGen have stalled, however, demonstrating that there are limits to actualizing an integrated model when it entails cross-border collaboration (Bronskill, 2013).

A high-profile case illustrating the involvement of integrated investigative teams in the attempt to prevent terrorism is the Via Rail plot of 2013. According to media and police reports, "Project Smooth" was an international investigation coordinated by the Montreal and Toronto INSETs working together with the FBI, Citizenship and Immigration Canada, Transport Canada, and, apparently for the first time, the para-police forces of VIA Rail and CN Rail (Anonymous, 2013, interview, 28 October; Government of Canada, RCMP, 2014b). Together, these organizations claimed that they had thwarted plans to attack a Via Rail train travelling between Toronto and New York and declared the operation a resounding success. Moreover, the RCMP specifically promoted the fact that the

tip originally came from the "Muslim community" and contacted 22 Muslim leaders for a briefing before the press conference that announced the arrests to the public (Canadian Press, 2013). This demonstrates another facet of integration highlighted in *Building Resistance*: the importance of citizens in contributing to national security with the goal of resilience. According to the strategy, "citizens also have a responsibility to act—a responsibility to work with Government and security personnel, and a responsibility to build strong and supportive local communities" (Department of Public Safety, 2013, p. 6). Although the Via Rail cases are still before the courts, and the RCMP argue that there was "no imminent threat," the attention the RCMP drew to the role of integration specifically in this instance suggests the importance the Canadian government places on the model.

Respond: emergency management integration

The final pillar of the counter-terrorism strategy focuses on the responses of authorities and emergency management officials in the event that a terrorist attack occurs. The strategy explicitly notes that officials will "respond proportionately, rapidly, and in an organized manner to terrorist activities and mitigate their effects" (Department of Public Safety, 2013, p. 21). The focus on post-event emergency management priorities is emerging in the context of an increasing recognition that disrupting potentially violent networks through intelligence-led strategies is a far from simple enterprise. There is no such thing as perfect security, and maintaining heavily fortified areas, often designated as critical infrastructure, always leaves open the prospect for an attack in an adjacent area. In spite of the unlikelihood of a terrorist attack occurring, governments are consistently developing capacities for a rapid and organized response to a terrorist attack or potential disruption so as to best mitigate any untoward effects (Department of Public Safety, 2013). Such preparations center on the key organizing metaphor of resilience, so that in the event of an attack, responders can provide support to affected Canadians, protect Canadian interests and minimize the impact of terrorist activity so that "Canada can quickly return to the routines of ordinary life" (Department of Public Safety, 2013, p. 23). Integration is therefore a cornerstone of resilience policies that are developed to remediate crisis situations. Much of the integration in the realm of emergency management occurs between law enforcement, city officials, ambulance, fire, and other first responders, as well as specially equipped emergency response teams (ERTs) and medical and health officials. In addition, the role of training exercises at major events that prepare officials for a chemical, biological, radiological or nuclear explosive (CBRNE) attack often draw together the capabilities and resources of a wide range of first-responders.

However, notwithstanding the move toward resilience, it is important to recall that the actual number of terrorist attacks that have occurred in the US and Canada are statistically extremely low as compared to other causes of injury or fatality. In 2012, police reported 114 "terrorism related incidents," over 60 percent of which were hoaxes (Statistics Canada, 2013). The Global Terrorism

Database records 17 attacks on Canadian soil between 2001 and 2011—most of which resulted in no injuries, and only one of which resulted in a fatality, which was ruled a suicide by the police (National Consortium for the Study of Terrorism and Responses to Terrorism, 2012). Fewer than 40 people have been charged under Canada's anti-terrorism legislation; 14 have been convicted (Government of Canada, Department of Justice, 2001; Shen, 2014; "The Government of Canada's response to the terrorist attacks of 9/11," 2013). Figures for attacks are similarly low in the United States, where the database records 183 attacks between 9/11 and 2011, including attacks by environmental, animal rights and anti-abortion activists. Again, most of these attacks resulted in no injuries or fatalities; there have been 37 terrorism-related deaths on American soil since 9/11 (National Consortium for the Study of Terrorism and Responses to Terrorism, 2012). However, when attacks have happened, they provide a novel opportunity for evaluative assessments to determine the relative effectiveness of the response. In addition, post-incident preparations for terrorist related attacks can also be leveraged into emergency responses for natural disaster scenarios in an "all-hazards" approach.

Interestingly, after 9/11, information hiving was widely viewed as the primary shortcoming that led to the attacks, and the solution of integration was subsequently understood to enhance capabilities and practices of information sharing. By comparison, with a post-incident scenario after the Boston Marathon bombing, much of the focus was on how city officials, law enforcement, emergency responders, military officials, the FBI, medical personnel and citizens responded to the downtown bombings (Gawande, 2013). As in the Via Rail case, integration was touted by security officials as key to the operation's success. Shortly after the suspect was apprehended, the Boston Police tweeted: "How do we spell team? We spell it like this: BPD, FBI, ATF, MSP, MBTA, WPD, ICE, NEMLEC, EMS, BFD, MIT, SWAT and YOU. We r #BostonStrong" (Boston Police, 2013).

It is tempting to point toward failings at the level of "prevent" and "detect," but the Boston Marathon bombings do provide an interesting test case to examine integration in a post-disaster scenario. Three deaths occurred in the wake of the downtown blast, and more than 170 people sustained injuries, many of them very serious. Coping with the dramatic increase in the number of individuals with serious injury placed an immense strain on first responders and hospital staff. Command structures and tactical plans were in place to minimize the damage from such events; however, even with formalized emergency management policies in place, officials insisted that the rapid pace of the unfolding events meant that mobilizing medical personnel according to any ritualized plan was not possible (Gawande, 2013). Officials were forced to move faster than previously established protocol could successfully accommodate if they were to treat the wounded efficiently. Under critical constraints, first responders and other medical officials often took it upon themselves to break into "trauma teams" for each individual patient where possible. The emergency management response, and particularly the response in the first responder and medical

communities, raises important considerations on the value of reality-based training exercises as a means to develop and hone integrated capacities in emergency management, over and above more formalized logistical planning in emergency management policies.

Major events, given their vast logistical requirements, also have led to significant cooperation between civilian and military officials. During the lead-up to the Vancouver 2010 Olympics, the creation of the Vancouver Police Department (VPD) Military Liaison Unit (MLU) was intended to facilitate integration between civilian police forces and members of the DND/CF. Again anticipating future disaster scenarios, the purpose of the VPD MLU is to facilitate joint communication efforts between previously distinct institutions. Drawing on the experience of military personnel in the Vancouver Police Department, the VPD MLU is able to facilitate a common operational language as well as resolve previously murky jurisdictional considerations that might emerge if, and when, the DND/CF are operating in Canadian cities (Molnar, 2014). Since these initial partnerships have formed, however, the MLU has developed extensive partnerships with the US Army and the Washington National Guard, among other US military organizations, and they regularly participate in reality-based joint training operations (Molnar, 2014).

Integration: to what effect?

There is certainly some evidence that integration has had positive effects. Perhaps the most significant and direct positive outcome is in the area of enhanced emergency management preparations and response. In emergency management conditions, the value of preparing for crisis scenarios applies to both natural disaster and terrorist attack scenarios; such preparation can mitigate the extent to which human and infrastructural damage may occur under either of these conditions. Interestingly, however, as the Boston Marathon bombing event showed, even contingency policies on paper are no replacement for the value and experience gained through joint-training exercises and mock drills (Molnar, 2014). However, in the context of intelligence-led policing as a primary aspect of counter-terrorism policy, unintended risks as well as benefits may be associated with the move toward integration.

Formalizing previously informal networks means that cooperation is increasingly conducted according to formalized rules and agreements, which are intended to maximize the oversight of important intelligence details. In some cases, the process of formalization creates new rules that can make cooperation easier: for instance, amending the Export and Import Permits Act to allow members of Shiprider teams to cross the border with their duty weapons also solved a longstanding irritant wherein police or Coast Guard vessels in Canada and the United States effectively broke the law when the only maritime route between two points in one country was through the national waters of the other (Anonymous 2014, interview, 22 July). Structured cooperation may give security actors more confidence that the right players are involved (Anonymous 2013,

interview, 28 October). As individuals change jobs, more structured cooperation can help preserve institutional memory. Seconded individuals who return to their home organization may return with important new skills and contacts. However, as Benoît Dupont argues (see Chapter 9 of this volume), the premise that it takes a network to fight a network may not be based on a sound understanding of how policing organizations work. Beyond Dupont's argument, we argue that there are several other reasons why the integration of people and information may not be the solution that post-9/11 security discourse has made it out to be.

First, integration and collaboration are not a panacea. While there are several examples of potential terrorist attacks thwarted, such as the Via Rail plot, that have been attributed to the role of integrated units and information, there are others—such as the Boston Marathon bombing in 2013—where terrorist attacks succeeded in spite of very strong integration before the event. While most proponents of integration would acknowledge that there is no such thing as perfect security, many of the efforts to prevent and detect terrorism are premised on the idea that with better integration will come an improved capacity for stopping terrorist attacks before they happen. Accordingly, the Canadian Criminal Code refers to the offences of "enhancing" or "facilitating" terrorist activity—slippery terms that necessitate investigating individuals, their intentions and their connections (Department of Public Safety, 2013). Terrorist acts are low-probability events, which makes it nearly impossible to find patterns predicting when and where they will happen and who will commit them. They do not cost very much, and the tools necessary to carry them out—a pressure cooker in the case of the Boston Marathon bombing—may be indistinguishable from tools people use in their everyday lives. The pressure on governments to create a zero-risk, high-security environment—an impossible task—also creates pressure to gather more and more data about citizens generally and to share it across more and more agencies. The rational calculation of risks in such situations becomes nearly impossible because rational calculation no longer makes sense, particularly in the absence of any valid benchmark statistics on terrorism as a quantifiable, knowable and therefore predictable event. Aradau and van Munster argue that we have to take into account the fact that risks are socially constructed. They are not objectively "out there" to be known or not known. Rather, we render them calculable and knowable by the ways we think about them (Aradau and van Munster, 2007). Depending on how we think about terrorism—and what kinds of acts we argue constitute "radicalization" and "facilitating" or "enhancing" terrorist capabilities, risk calculations will look different.

Integration has the goal of bringing together information from different parts of the security bureaucracy and even from different countries. We are promised that this increased surveillance will increase the government's ability to stop terrorist attacks. This may be based on faulty assumptions about the possibility of identifying potential terrorists and precursor behaviors to attacks; the result may be that we are inundated with an over-abundance of intelligence information such that successful analysis is made increasingly difficult. As one security official noted, we may not have a problem of finding a needle in a haystack or of

connecting the dots, but rather of identifying two or three grains of sand from a pile with the wind blowing through it (Anonymous 2013, interview, 28 October).

Moreover, even if it is possible to predict terrorism, the model of integration described here assumes that the information being sought is in one of the databases being integrated. Integration may solve the problem of information being in different places, but it cannot solve the problems related to the quality of actionable intelligence or the lack thereof. Resources are finite, and if an individual generates only low-level suspicion, an investigation is unlikely to be prioritized (Savage, 2011). Robust integration had very little to do with the fact that American security officials did not identify Djokar Tsarnaev, the perpetrator of the Boston Marathon attacks, as a threat despite the fact that his name was in various counter-terrorism databases. The assessment of Tsarnaev's threat was one of a thousand conducted in 2011 by the Boston Joint Terrorism Task Force, so there is little surprise that not all pieces of information were given equal priority (Shane and Schmidt, 2013). However, even infinite resources would not make detection in integrated databases perfect. If an individual has not previously done anything that makes them sufficiently suspicious as to warrant further investigation, he or she is unlikely to be further investigated.

For an integrated system to work, systems designed to integrate information must work as designed. This is not always the case. Counter-terrorism has a big data problem. As mentioned, it turns out to be difficult to write predictive algorithms on the basis of a low-occurrence event such as terrorism (Citron and Pasquale, 2011). Planned systems must also be implemented. A recent report from the Office of the Director of National Intelligence concluded that many American fusion centers, which are integrative institutions designed to gather intelligence data from different sources, do not have mechanisms for incorporating data gathered in Suspicious Activity Reports (SARs) into their intelligence workflow (Perera, 2013a). A hearing into intelligence sharing preceding the Boston Marathon bombing revealed complaints from the Boston Police that information sharing flowed one way, from local to federal (FBI) officials, but not the other way (Perera, 2013b). While these examples come from the United States, the general argument that integration creates complexity in the implementation of policy still stands. Integration does not necessarily lead to efficiency.

A second problem with integration is that it creates complexity that may lead to accountability problems. Research about bureaucracies suggests that individuals feel less responsibility for the outcome of a policy action if they cannot see it. In a network, this dissipated causality may be exacerbated as information is shared through a network (O'Toole, 1997). While co-locating individuals may help to develop the trust needed to create the mutual expectations that experts suggest are necessary for accountability in a network (O'Toole, 1997), the sheer growth of integrated security networks as described above may make the development of such norms difficult. The complexity created by integration may also

reduce accountability as information is shared between representatives of different agencies in integrated institutions. Like a game of broken telephone, information is interpreted and possibly distorted by each successive agency that sees it, making errors more difficult to correct and increasing the likelihood of catching an innocent person in the web of an investigation. In addition, the extent of this accountability also extends between intelligence authorities and the public. In the "Five Eyes" SIGINT arrangement, it is often not clear under what jurisdiction specific intelligence has been collected, which raises some concerns over the legal legitimacy of specific practices of intelligence collection (Privacy International, 2013).

Integration may also lead to the problem of regulatory arbitrage, in which activities are shifted to the jurisdiction or body with the most lax regulatory regime, or in which actors otherwise use differences in the rules between jurisdictions to do things they would not otherwise be permitted to do (Citron and Pasquale, 2011). Under circumstances where Five Eyes partners can "legally" collect (and share) intelligence on each other's behalf, regulatory arbitrage allows the circumvention of laws designed to protect against unreasonable domestic spying. It may happen in the domestic intelligence community as well; the Federal Court has recently ruled that CSIS has "breached duty of candour" by not telling the Federal Court that Five Eyes allies would be used in an international terrorism investigation with two Canadian suspects when it requested assistance from CSE (Freeze 2013). So while the request for assistance is allowed within the law, CSE also seems to have been counting on an integrated network to provide additional information beyond what would typically be allowed.

Conclusion

Integration is one of the most prevalent but least studied trends in the security sectors of major democracies. Its prevalence is born of a lesson learned after 9/11 that connecting the dots will prevent terrorism, and of models of intelligence-led policing that focus on gathering and analyzing information in the service of preventing crime. An examination of the trends toward integration in Canada suggests that it has significantly changed the way national security is conducted. Integration has led Canadian security authorities to seek new partnerships within and outside Canada. Security networks stretch to include authorities at all levels of government, foreign partners, private citizens tasked with preventing radicalization and reporting suspicious activities, and firms that may provide services or take on the burden of securing themselves. Clear boundaries between domestic and international and between public and private are dissolved as security threats are conceptualized as coming from radicalized individuals in Canada, rather than from abroad. The difficulty of identifying individuals who may commit violent acts, together with the increased capacities for surveillance generated by integrated partnerships in information sharing, has meant that personal data travels further, in increasingly cohesive packets, than it ever has

before (Haggerty and Ericson, 2000). In Canada, the recommendations emerging from the O'Connor Report on Canadian complicity in Maher Arar's rendition to Syria have resulted in some centralization of information sharing in an attempt to exercise some control over information. However, recent stories about intelligence cooperation in the Five Eyes alliance suggest that regulatory arbitrage to circumvent such safeguards is not unheard of.

Integration has also led to innovation. Better cooperation in leveraging emergency management situations has prompted the increasing use of smaller "trauma teams" as an important disaster response mission-based initiative. Furthermore, integration at the Canada–United States border has led to substantial innovation, with integrated teams being developed that bring together Canadian and American security authorities in increasingly significant ways. If NxtGen, the land-based extension of Shiprider, is ever to fully materialize, it will mark unprecedented cooperation between Canada and the United States in pursuit of national security. Similarly, the integrated model of security arguably provided the structural conditions for both the emergence of the Vancouver Police's MLU and its innovative activities in training with American armed forces. The fact that the VPD conceptualizes itself as requiring military skills, but also the fact that it has the deep partnerships required to refine them, are a direct consequence of the increased integration between military and police partners and the concurrent dissolution of the boundaries between crime-fighting and security.

Integration is not the first, nor will it be the last, organizational policy trend to seize the imagination of governments keen to improve their efficiency and protect citizens. However, as with all such trends, careful reflection on their promise and peril is imperative—we should not assume that we have learned the right lessons from experience or that our lessons will not have unexpected consequences. Research on integration in Canada and the United States suggests that conclusions about efficiency and success may not be borne out, and that consequences for citizens and accountability are mixed.

Notes

1 Italics added.
2 We focus in this chapter specifically on intelligence-gathering partnerships in official strategies aimed at preventing "radicalization," as other chapters in this volume discuss the prevention of radicalization more generally.
3 According to the RCMP, the SPROS database is "the new National Security Program's primary database for the electronic storage, retrieval and management of national security criminal investigations and information, and on a required basis, classified criminal intelligence and other sensitive cases."
4 It is important to note that CSE's collecting has, for ostensible national security reasons, extended beyond these more rigid rules imposed upon CSIS and the RCMP. Given the existence of "Mandate C" that stipulates assistance to lawful access procedures on behalf of CSE to both CSIS and the RCMP, these findings and the regulatory conditions that extended from them are "legally" able to be undermined.

References

Apuzzo, M. and Goldstein, J. (2014) New York drops unit that spied on Muslims. *New York Times.* 15 April.

Aradau, C. and Van Munster, R. (2007) Governing terrorism through risk: Taking precautions, (un)knowing the future. *European Journal of International Relations* 13, pp. 89–115.

Boston Police (2013) How do we spell team? We spell it like this: BPD, FBI, ATF, MSP, MBTA, WPD, ICE, NEMLEC, EMS, BFD, MIT, SWAT and YOU. We r #BostonStrong. 22 April. Twitter post.

Bronskill, J. (2013) Canada–U.S. border: American police want legal exemptions, RCMP says. *Huffington Post.* 31 July.

Canada–United States Cross-Border Crime Forum (2011) *Cross-Border Crime Forum: Next Generation Operations*. 28 October. Washington DC.

Canadian Access to Social Media Information (CATSMI) Project (2013) *Using Social Media Information.* Available at: www.catsmi.ca/authorities/using-social-media-information. Accessed 26 July 2013.

Canadian Association of Chiefs of Police (2004) *Resolutions Adopted at the 99th Annual Conference.* Vancouver: Canadian Association of Chiefs of Police.

Canadian Association of Chiefs of Police (2007) *Resolutions Adopted at the 102nd Annual Conference*. Calgary: Canadian Association of Chiefs of Police.

Canadian Press (2013) Suspects charged in Via train terror plot have Al-Qaida ties: RCMP. *Macleans.ca.* 22 April.

Citron, D. K. and Pasquale, F. (2011) Network accountability for the domestic intelligence apparatus. *Hastings Law Journal.* 62, pp. 1441–2011.

Communication Security Establishment Canada (CSEC) (2007) OPS-1–11 Retention Schedules for SIGINT Data.

Federal Court (Canada) (2013) *X (Re).* FC 1275. 22 November.

Freeze, C. (2013) How CSEC became an electronic spying giant. *The Globe and Mail*. 30 November. Available at: www.theglobeandmail.com/news/politics/how-csec-became-an-electronic-spying-giant/article15699694/?page=all.

Freeze, C. (2014) Spy agency's work with CSIS, RCMP, fuels privacy breaches. *The Globe and Mail.* 31 January. Available at: www.theglobeandmail.com/news/politics/spy-agencys-work-with-csis-rcmp-fuels-fears-of-privacy-breaches/article16623147/.

Gawande, A. (2013) Why Boston's hospitals were ready. *New Yorker Magazine.* 17 April.

Government of Canada, CSIS [Canadian Security Intelligence Service] (2014) 2011-2013 Public Report. Available at: www.csis.gc.ca/pblctns/nnlrprt/2011-2013/index-en.php. Accessed 27 January 2014.

Government of Canada, Department of Justice (2001) About the Anti-terrorism Act 15 October. Available at: www.justice.gc.ca/eng/cj-jp/ns-sn/act-loi.html. Accessed 31 July 2014.

Government of Canada, Department of Public Safety (2013) *Building Resilience Against Terrorism*.

Government of Canada, RCMP [Royal Canadian Mounted Police] (2013a) Canada–U.S. Shiprider. 25 June. Available at: www.rcmp-grc.gc.ca/ibet-eipf/shiprider-eng.htm. Accessed 16 August 2014.

Government of Canada, RCMP (2013b) RCMP arrests two individuals for terrorism-related charges. 22 April. Available at: www.rcmp-grc.gc.ca/news-nouvelles/2013/04-22-ns-sn-eng.htm. Accessed 6 December 2013.

Government of Canada, RCMP (2014a) Integrated Border Enforcement Teams (IBETs). 3 March. Available at: www.rcmp-grc.gc.ca/ibet-eipf/index-eng.htm. Accessed 16 August 2014.

Government of Canada, RCMP (2014b) Integrated National Security Enforcement Teams. Available at: www.rcmp-grc.gc.ca/secur/insets-eisn-eng.htm. Accessed 16 March 2015.

Haggerty, K. and Ericson, R. V. (2000) The surveillant assemblage. *British Journal of Sociology*. 51, pp. 605–622.

Kehl, D. (2014) *Surveillance Costs: The NSAs Impact on the Economy, Internet Freedom and Cybersecurity*. New America's Open Technology Institute. Policy Paper. July.

Lippert, R. and O'Connor, D. (2006) Security intelligence networks and the transformation of private security. *Policing and Society*. 16, pp. 49–65.

Molnar, A. (2013) In the shadow of the spectacle: The security and policing legacies of the Vancouver 2010 Olympics. Doctoral dissertation, University of Victoria.

Molnar, A. (2014) The geo-historical legacies of urban security governance and the Vancouver 2010 Olympics. *Geographical Journal*. DOI: 10.1111/geoj.12070.

Monaghan, J. and Walby, K. (2012) Making up "terror identities": Security intelligence, Canada's Integrated Threat Assessment Centre and social movement suppression. *Policing and Society*. 22 (2), pp. 133–151.

National Consortium for the Study of Terrorism and Responses to Terrorism (START) (2012) Global Terrorism Database [Data file]. Available at: www.start.umd.edu/gtd.

Office of the Privacy Commissioner of Canada (2009) Workshop on Privacy, Security, and the Vancouver 2010 Olympics (Program Report). Office of the Privacy Commissioner of Canada.

O'Toole, L. J. (1997) The implications for democracy in a networked bureaucratic world. *Journal of Public Administration Research and Theory*. 7 (3), pp. 443–459.

Perera, D. (2013a) Suspicious activity reports use in fusion centres limited by technology. *Fierce Homeland Security*. 5 September. Available at: www.fiercehomelandsecurity.com/story/suspicious-activity-report-use-fusion-centers-limited-technology/2013-09-05?utm_medium=nl&utm_source=internal. Accessed 12 May 2013.

Perera, D. (2013b) Boston police commissioner decries lack of info sharing from Feds. *Fierce Homeland Security*. 14 July. Available at: www.fiercehomelandsecurity.com/story/boston-police-commissioner-decries-lack-info-sharing-feds/2013-07-14. Accessed 6 December 2013.

Privacy International (2013) Eyes Wide Open: Special Report.

Privy Council Office, Government of Canada (2004) *Securing an Open Society: Canada's National Security Policy*.

Privy Council Office, Government of Canada (2005) *Securing an Open Society—One Year Later: Progress Report on the Implementation of Canada's National Security Policy*.

Savage, C. (2011) F.B.I. casts wide net under relaxed rules for terror inquiries, data shows. *New York Times*. 26 March.

Shane, S. and Schmidt, M. S. (2013) Boston police weren't told F.B.I. got warning on Tsarnaev. *New York Times*. 9 May.

Shen, A. (2014) Canadian "poised to become terror tourist" given 10-year sentence. *The Globe and Mail*. 24 July.

Statistics Canada (2013) Police-reported crime statistics in Canada, 2012. Available at: www.statcan.gc.ca/pub/85-002-x/2013001/article/11854-eng.htm?fpv=269303. Accessed 25 July 2013.

Steinbachs, J. (2001) Police forces team up. *Ottawa Sun.* 31 October.
Thacher, D. (2005) The local role in homeland security. *Law and Society Review.* 39, pp. 635–676.
Woods, A. (2002) Four antiterror squads launched. *The Globe and Mail.* 18 June.
Zedner, L. (ed.) (2009) *Security: Key Ideas in Criminology*. London: Routledge.

11 A systematic approach to developing a computational framework for counter-terrorism and public safety

Andrew J. Park and Herbert H. Tsang

Introduction

Terrorism refers either to a doctrine about the effectiveness of a tactic of fear-generating, coercive political violence, or to a practice of calculated, direct violent action for its propagandistic and psychological effects on various audiences by targeting mainly civilians and non-combatants (Schmid, 2012). It has taken place since ancient times. Terrorism used to be constrained into local geographical areas (Primakov, 2004), so that governments were mostly concerned with threats occurring within their own borders. However, as exemplified most notably by the attacks of on 9/11, among many others (including the recent rise of ISIS), contemporary terrorism is global in scope. Many Western countries devised their counter-terrorism strategies in reaction to the 9/11 attacks, showing convergence in both objectives and terminology. The United States has a four-pillar foundational counter-terrorism approach: defeat, deny, diminish and defend (Brooks, 2010). The strategy aims to reduce terrorist activities by decreasing the scope and capability of terrorists. The United Kingdom has also developed their counter-terrorism program with the strategies of prevention, pursuing, protecting and preparing (Brooks, 2010). These strategies challenge the ideology of violent extremism and aim to disrupt and stop promotion and recruitment by violent extremists. The Canadian government has taken similar initiatives to counter terrorism (see Chapter 10 by Kitchen and Molnar in this volume). In order to ensure the safety and security of its citizens, Canada developed a framework to build resilience against terrorism by reinforcing four strategic elements: prevent, detect, deny and respond.

Clearly, it is a priority to detect terrorist threats and prevent them from happening. However, when a terrorist attack occurs, it is important to respond rapidly and in an organized manner to save lives, reduce personal injuries, and mitigate the damage of such an attack. This kind of immediate and coordinated response requires careful planning and protocols, with the participation of local law enforcement and emergency management authorities. At the same time, incorporating currently available technologies in these strategic response plans and protocols opens a new way to handle chaotic incidents in an effective and systematic manner.

Counter-terrorism initiatives aim at developing effective and efficient strategies and tools in order to prepare against, prevent, and respond to a wide variety of terrorist threats, including chemical, biological, radiological, nuclear and explosive (CBRNE) threats. As such, governments and security agencies have been actively trying to improve their capabilities by funding and supporting innovative science and technology approaches that address national public safety and security needs and provide tools for CBRNE response and preparedness.

This chapter presents an overview of the computational framework that we have developed—the GENIUS system (Tsang *et al*., 2010; Park *et al*., 2012). GENIUS is a framework which provides decision support, response planning and risk assessment. The framework helps devise CBRNE response plans and preparedness through several components: (1) a parametric-based human behaviors modeling module, (2) a human behaviors simulation module, (3) a flexible virtual environment module which we have been using to study human behaviors in a controlled environment, and (4) a visualization module that can integrate with both a commercial GIS system and a 3D virtual environment. These modules are all integrated together in order to provide a system that is both modularized and flexible. Because the GENIUS system is modularized, it can easily incorporate state-of-the-art technologies available today.

Emergency preparedness for terrorism

Preparing for an emergency caused by terrorism is not the effort of a single government entity. It is rather a collegial effort of every organization and department involved with such emergency preparedness. This includes federal and local emergency management authorities, law enforcement, military, medical emergency teams, and policy-makers. Perry and Lindell (2003a) conducted an extensive study on emergency preparedness for terrorism based on literature for natural and technological disasters. They argue that emergency preparedness, in particular emergency preparedness within a community, requires planning, training and written plans. There is an obvious difference between natural and technological disasters and disasters caused by terrorism. For example, any disasters caused by CBRNE will generate higher and more acute levels of fear than other kinds of disasters. However, there are enough similarities between them for well-studied and well-established emergency preparedness for natural and technological disasters to be a good foundation for counter-terrorism preparedness.

Some of the guidelines by Perry and Lindell for emergency planning are of particular interest in developing a computation framework for counter-terrorism. Their first guideline reads, "It should be based upon accurate knowledge of the threat and of likely human responses" (2003a, p. 340). It is important to obtain knowledge of different terrorism threats (such as CBRNE) and their characteristics. At the same time, it is equally important to know how people respond and behave when they are attacked by terrorists. It is common for emergency

managers to think that people panic, become irrational, and flee when a disaster occurs. However, research shows that most people make their own decisions about whether or when to evacuate. Some even stay longer to search for survivors, assist the injured, and try to protect property from further damage. This kind of knowledge helps emergency managers and other relevant authorities to devise an emergency plan accordingly.

However, patterns of evacuation and fleeing can be very different for terrorist attacks. One of the principal activities of managing an emergency caused by terrorism is population protection (Perry and Lindell, 2003b). One of the actions to protect population is to move those at risk away from threat by prompt evacuation. This is an important action taken by first responders, which is incorporated into our computational framework.

Another guideline of Perry and Lindell imposes an idea that emergency plans should have a training component (2003a). The training component plays the role of informing officials, public administrators, and citizens on what to do in case of an emergency. Another role of the training is to increase the effectiveness of emergency response. Our computational framework incorporates this training component in emergency preparedness and develops a first responder training program using virtual reality technology.

A computation framework for counter-terrorism

Human behavior study using virtual environments

In our previous study, a series of research experiments were conducted to discover patterns of human behaviors and responses in urban environments and, in particular, the behaviors and responses that are influenced by the fear and perception of crime (Park *et al*., 2010, 2011). These experiments made use of virtual environments to avoid ethical issues for participants. In addition, the use of virtual environments has become affordable, efficient, portable and reliable.

Different virtual environments were used for the experiments. Some virtual environments resembled the corresponding real environments, while others looked realistic but were made for the purpose of experiments. From the results of our previous experiments and a literature review of the social sciences (LaGrange *et al*., 1992; Hanyu, 1997; Sampson and Raudenbush, 1999; Hanyu, 2000; Herzog and Flynn-Smith, 2001; Weinrath *et al*., 2007), greater knowledge about patterns of human behaviors influenced by fear has been gained. For example, most people are afraid of social incivilities (prostitution, drug dealing, panhandling, public drunkenness or homelessness) more than physical incivilities (litter, broken windows, abandoned storefronts, unkempt lots, graffiti or vandalism). We have since incorporated our findings on fear-influencing human behaviors into our computational framework. Virtual environments have proven to be excellent research tools to systematically study human behaviors in various situations with tight controls of experimental variables.

GENIUS

Agent-based modeling

Based on our previous study, a computational framework (GENIUS) was developed to investigate human behaviors in urban environments. The goal is to capture the complexity and diversity of human behaviors in a robust and systematic way. In the course of developing this framework using agent-based modeling (ABM) techniques, a methodological framework and a tool environment were developed to address the needs and challenges of modeling complex behaviors. ABM is a class of computational models that simulate the actions and interactions of autonomous agents with each other and the environment (Bonabeau, 2002). This approach is based on the idea that a system is composed of decentralized, individual agents and that each agent interacts with other agents and the environment according to localized knowledge and rules. The goal of the model is to re-create and predict the appearance of complex phenomena based on the simulation of the simultaneous operations and interactions of multiple agents. The process is one of emergence from the lower (micro) level of systems to a higher (macro) level. As such, a key notion is that simple behavioral rules generate complex behaviors.

GENIUS has an agent behavior engine which was constructed using the swarm intelligence (SI) paradigm (Kennedy and Eberhar, 1995). The expression swarm intelligence was first introduced by Beni and Wang (1989) in the context of cellular robotic systems. Since then, SI has been successfully applied in many areas, including forecasting pedestrian evacuation times (Izquierdo *et al*., 2009), diagnosis of human tremor (Eberhart and Hu, 1999), and a variety of optimization applications. SI is a decentralized and self-organized system where the collective behaviors of agents interacting locally with their environment cause coherent functional global behaviors. Typically, these agents are unsophisticated and global patterns emerge from their collective behaviors. SI relies upon countless interactions between individual agents, each of which is following simple rules of thumb. By computing and describing the space–time behavior of individual pedestrians in a microscopic model, we can observe characteristics of the flow rather than individual pedestrians. This allows us to study not only the behaviors and decisions of individual pedestrians but also their interactions with other pedestrians in the crowd.

Specifically, there are different types of crowd behaviors. Forsyth defined crowds as “a temporary gathering of individuals who share a common focus of interest” (Forsyth, 2010, p. 503). He classified crowds into many different categories (see Figure 11.1). A casual crowd is a group people who happen to be in the same public or semi-public space at the same time. There is no common identity or long-term purpose among the people. A mob is defined as an acting crowd. Among mobs, there is a panic crowd who whose members are threatened and trying to escape from danger. In particular, the current GENIUS system simulates casual crowds and escaping mobs (panic crowds) models.

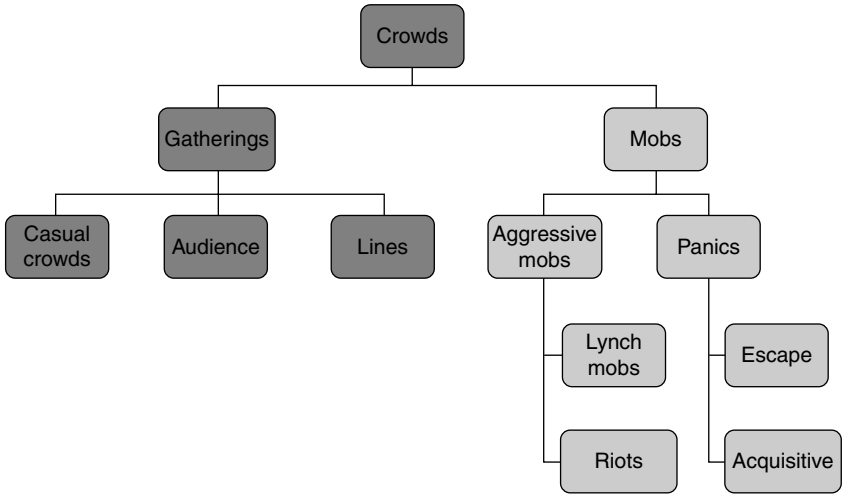


Figure 11.1 Classification of crowds (adapted from Forsyth, 2010).

Parametric modeling

Using a parametric model to model human behaviors is not new in the literature. Wakita and colleagues (2005) modeled the behaviour of a driver when following another vehicle. Parameters can be varied independently to modify a specific agent's behavior (e.g., walking speed, memory, decision rules, etc.). This authoring paradigm is highly flexible, allowing a wide range of applications. The entire set of parameters can be exposed individually for full low-level authoring control, or a subset of these parameters with constraints can be presented to a novice user for customization and personalization. In general, agents can be described by the following characteristics (Gilbert, 2008):

- Perception—the agents can perceive their environment and other agents in their vicinity;
- Performance—the agents have a set of behaviors that they can perform; often including motion, communication and action;
- Memory—the agents can record their perceptions of the previous states and actions;
- Policy—the agents operate using a set of rules, heuristics or strategies.

Higher-level constructs can be imposed on the basic parameter scheme by combining low-level parameters to create application-specific descriptive elements. In this way we have begun to build up a hierarchical library of behaviors and agent types which can all be combined and changed in any number of ways. In the highest level of the hierarchy of the GENIUS system, there are three types of

agent profile in our model: (1) civilian, (2) police and (3) terrorist, all of which behave differently. Furthermore, the second level of the agent's profile hierarchy can be refined using the following parametric qualities: age (small children, adult, seniors), gender (male and female) and personality (bold or fearful).

Users can define a number of agents with the same characteristics or create an agent with an individual profile separately. It was found in a previous study that people had different behavioral characteristics based on their gender and age (Park *et al*., 2010). Our framework incorporates these findings to create a large number of people with specific behavioral characteristics. Figure 11.2 shows the visualization of a crowd while the simulation is running.

In particular, three distinctive agents in the GENIUS system (civilians; police, either first emergency responder or security officer; and terrorists) have different behavioral characteristics. Civilian agents walk to their destinations. However, if there is any kind of terrorist attack (bombing, toxic gas or shooting), they try to escape from the dangerous zones. Police officer agents can be placed at strategic locations. When the terrorist attack occur, they quickly find and lead civilian agents who are around them to safety, or the closest exits if they are in buildings as police officer agents have good knowledge of the environment. Currently, terrorist agents are set to follow a pre-set path and shoot civilians and police officers on first sight (as in, for example, the Westgate Shopping Mall attack).

Emergency response plan and risk assessment using GENIUS

Various scenarios of terrorist attacks can be created and simulated in the GENIUS system. Environments (buildings and streets) can be created either by mouse clicks on the screen or by importing maps. Different attacks, such

Figure 11.2 The 3D visualization of a crowd in the GENIUS system.

as time bombs and/or toxic gases (biological threats), can be placed at different locations. In particular, toxic gases can be blown by the wind with a specific direction and strength. Different numbers of people (crowds) with customized parameters can be positioned in different locations. As the simulation runs, it will reflect and show how the crowd behaves when struck with a terrorist attack.

Agents of first emergency responders (police officers and emergency medical responders) can be strategically placed and simulated in the GENIUS system. Rescue missions can be carried out within the simulation. By varying the number and locations of these agents, the optimal emergency response plans and protocols can be devised to determine which can rescue the most people in the shortest time.

To verify and validate the framework, a set of simulation experiments with different emergency response plans was performed. First, a hypothetical environment and scenario were created in the GENIUS system. For the first experiment (Scenario A), 30 citizen agents were placed in a confined building where there were only four exits available. A bomb goes off inside the building and we expect our citizen agents to find evacuation routes.

The explosion of a bomb was simulated with realistic visualization and the behaviors of the people were animated in real time. Figure 11.3 shows the setup for the building and the agents. When the bomb went off, people panicked and tried to escape from the building. However, many of them could not find exits, and so they could not escape. After 100 cycles (time elapsed in the simulation), there were still 10 people inside the building. Figure 11.3b shows the number of people that escaped over that time. At 100 cycles, only 66.6 percent of the agents had escaped.

For the second experiment (Scenario B), four emergency responders were added to the same scenario. As shown in Figure 11.3c, they were placed at each of the exits. After the explosion of the bomb, these responders went into the building and led the people out of the building.

Figure 11.3d shows that 50 cycles after the bomb exploded, about 93 percent of the agents had escaped. Eventually all citizen agents escaped from the building after about 100 cycles, in contrast to the last scenario where only 66.6 percent of the agents had escaped at that point in time.

These two experiments show that the placement of emergency responders makes a big difference in evacuating people from a dangerous zone. One would expect these emergency responders to have complex knowledge of the environment and therefore to be able to provide more reliable information to the other agents in the crowd. However, these emergency responders operate under very simple rules. In terms of perception, they have better sight distance and wider peripheral vision angle than normal agents. They walk faster and, in terms of personality, they are bolder than normal agents. The operation rules are very simple as well. In case of emergency, when an emergency responder walks into the hot zone, their duty is to find people and lead them out of the hot zone. They repeat this cycle to try to find more people.

It was observed that with emergency responders in place, they could help civilians reach their destinations faster and more efficiently. This observation aligned both with our intuition and with previous research conducted by Pelechano and Badler (2006) on simulations of building evacuation. Their study also shows that a few trained leaders (first emergency responders for our study) can lead people out of the building quickly, increasing evacuation rates. However, too many leaders do not help decrease the evacuation time. Placing the appropriate number of trained leaders or emergency responders at strategic locations reduces the evacuation time and increases the evacuation rate.

Simulation of Boston Marathon bombings

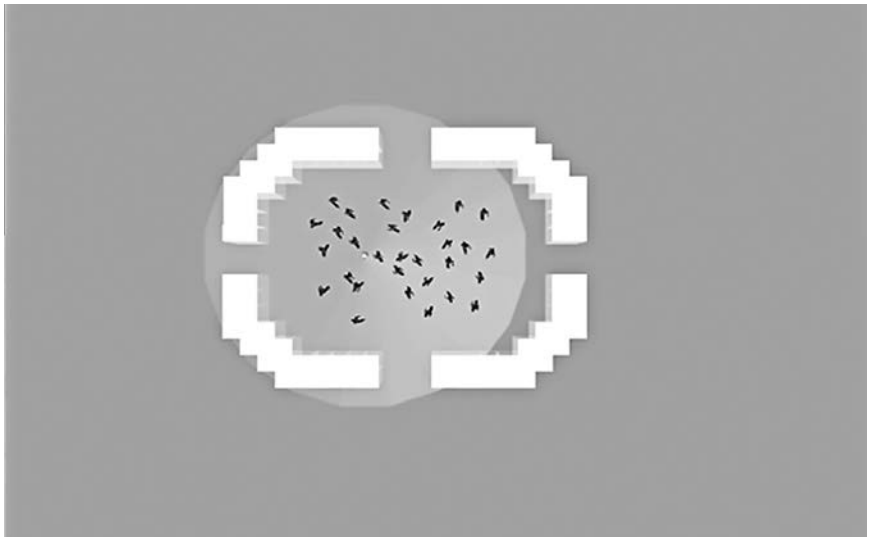
On 15 April 2013, two bombs were ignited among the cheering crowds near the finish line of the 117th Boston Marathon. The local hospitals received many casualties who had severe injuries caused by those explosions. Despite the nature and severity of the injuries, no patient who received hospital care died. Only three people were killed directly by the explosions before reaching a hospital. This very high survival rate was due to the brave and rapid response of first emergency responders and bystanders, the rapid transportation of injured patients, and the skilled hospital trauma teams (Walls and Zinner, 2013).

Considering the important role of first emergency responders, the Boston Marathon bombings were simulated within a realistic virtual environment using the GENIUS system. These simulation experiments are similar to experiments in the previous section. However, the GENIUS simulations were based on the real Boston bombing event. Figure 11.4a shows the simulation layout based on the physical environment of the real event (Figure 11.4b).

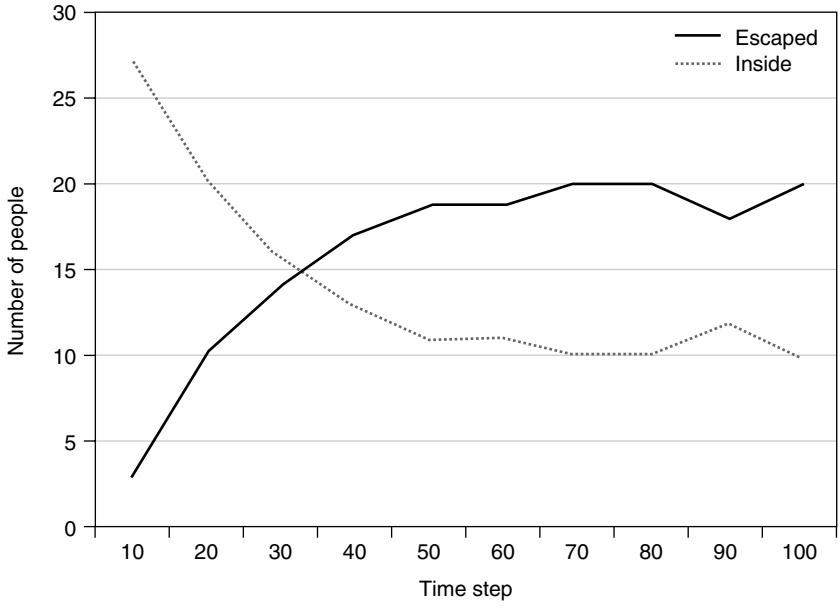
The first scenario (Scenario A) consists of only civilians without first emergency responders (police officers and emergency medical responders). Civilians were all over the streets. After the two bombs were ignited, crowds tried to escape from the bombed areas. Many of them were in panic, confused and uncertain where to go.

The second scenario (Scenario B) includes both civilians and first emergency responders. These responders were placed near the corners of buildings as they were strategic spots. They sought to rescue civilians by leading them out of the dangerous areas. Then the responders came back to the bombed areas, found more civilians, and led them to escape. They repeated this rescue mission until they had found everyone.

Figure 11.5 shows the comparison between the numbers of escapees over time in Scenario A and Scenario B. It clearly shows that with the help of first emergency responders, civilians can escape quicker than without any help during the first critical time right after the bomb explosions. The difference is largest between 15 and 45 seconds after the explosions.

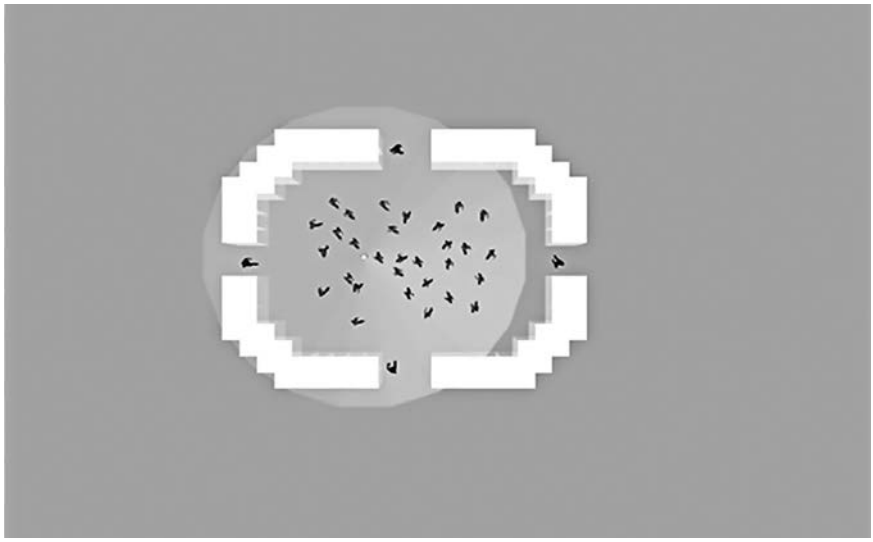


(a)

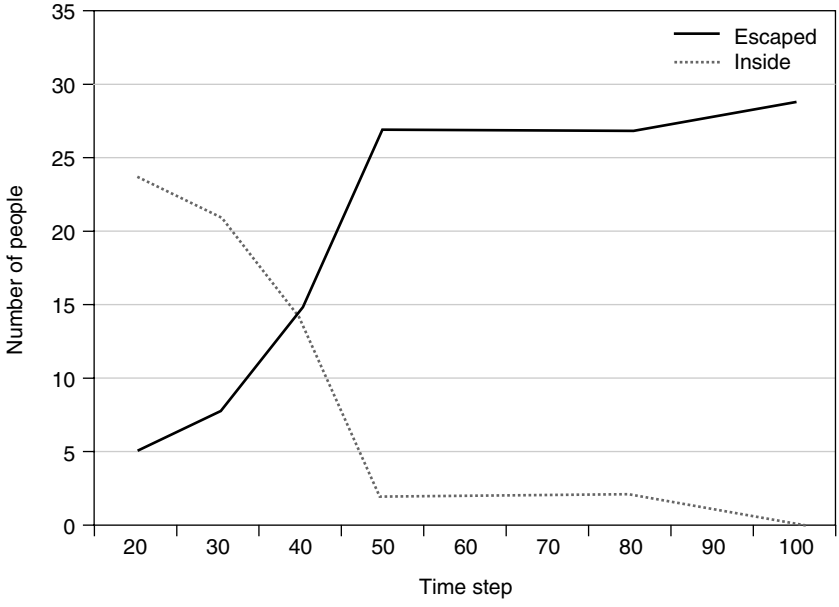


(b)

Figure 11.3 Initial setup and plots of a typical run in Scenarios A and B. The figures show (a) the setup of Scenario A (without emergency responders); (b) the number of escapees over time in Scenario A (without emergency responders); (c) the setup of Scenario B (with emergency responders); (d) the number of escapees over time in Scenario B (with emergency responders) (from Park *et al*., 2012).



(c)

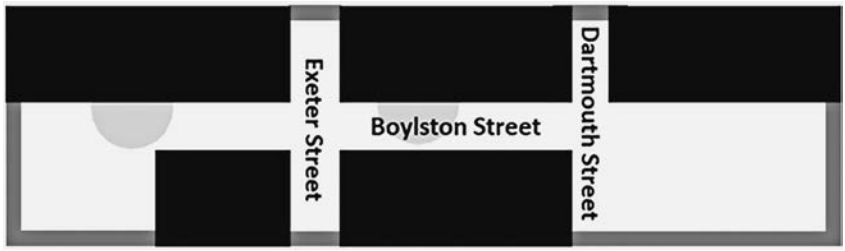


(d)

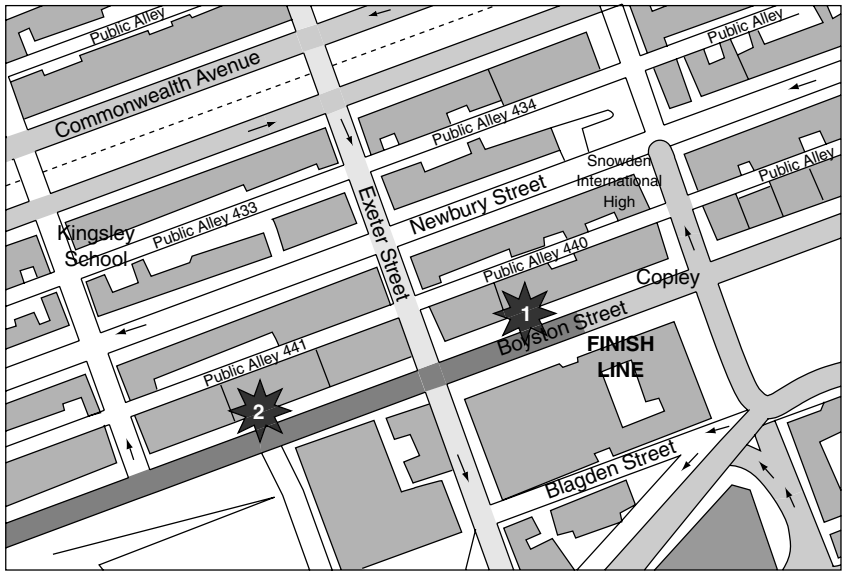
Figure 11.3 Continued

Westgate Shopping Mall attack

On 21 September 2013, 10 to 15 gunmen attacked the Westgate shopping mall in Nairobi, Kenya. They carried machine guns and AK-47 rifles and shot and hurled grenades at innocent shoppers and staff (Onuoha, 2013). The attack lasted for four days with heavy human casualties, killing at least 67 civilians, six security officers and five suspected terrorists, and injuring over 175 others. The Somali-based Al-Shabaab, a group that has ties to Al-Qaeda, claimed responsibility for the attack. They claimed that it was retribution for the deployment of the Kenyan military in Somalia.



(a)



(b)

Figure 11.4 The layout of the simulation of the Boston Marathon bombings: (a) the simulation layout of the Boston Marathon bombings; (b) the map showing the two bombing locations (data from Wikipedia: http://en.wikipedia.org/wiki/Boston_Marathon_bombings).

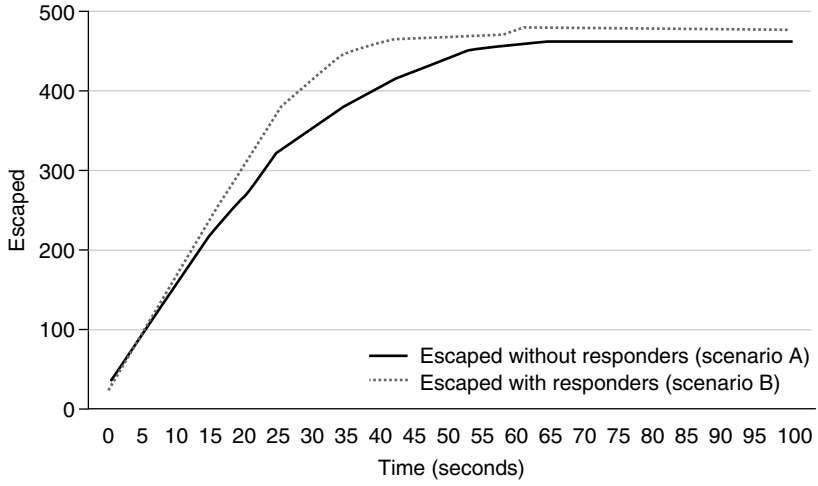


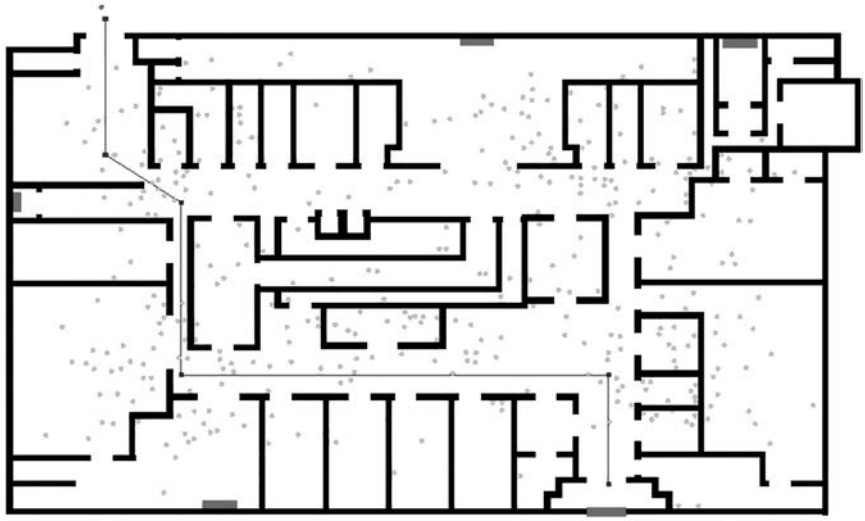
Figure 11.5 Simulations of the Boston Marathon bombings: graphs of the numbers of escapees over time in Scenario A and Scenario B.

The Westgate attack was not totally unexpected because Al-Shabaab had repeatedly warned that they would attack Kenya. A big shopping mall at the heart of Nairobi such as the Westgate mall could be a desirable target for terrorists to get international attention. If well-trained security officers could have been placed at strategic locations of the shopping mall they could have made a big difference in rescue efforts during the first few hours of the attack.

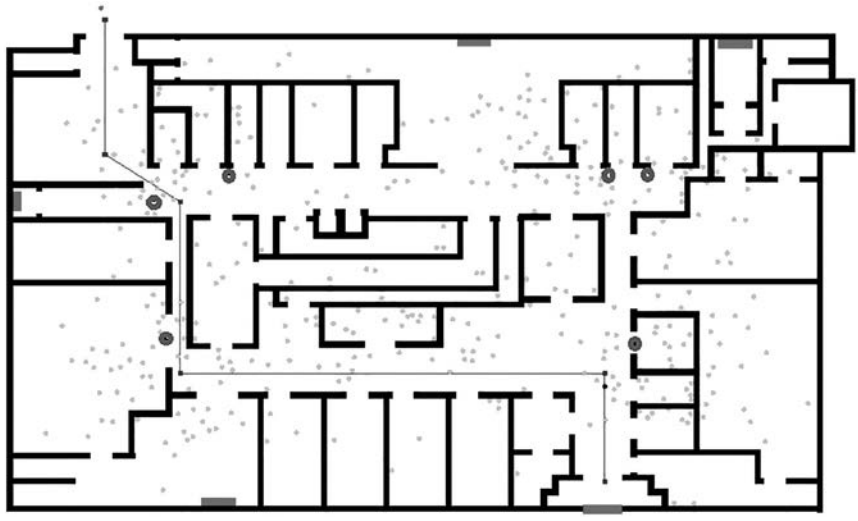
Using the GENIUS system, the Westgate Shopping Mall attack was simulated with the realistic 3D layout of the mall and two scenarios. The first scenario (Scenario A) depicts a terrorist attack without any well-trained security officers (Figure 11.6a). A gunman comes into the shopping mall from the rear entrance, shown at the left-top corner of the layout, and begins to shoot people (the red line shows the path of the gunman). People become panicked and try to run away from the gunman. However, many of them cannot find exits because of their panic and fear.

The second scenario (Scenario B) is the same as the first scenario except that well-trained security officers are placed at strategic locations of the mall (purple dots) (Figure 11.6b). These officers quickly act during the initial stage of the attack and lead people to close exits.

Figure 11.6c shows the comparison between the numbers of escapees over time in Scenario A and Scenario B. It is apparent that over the same time period many more people can escape with the help of well-trained security officers than without those security officers.

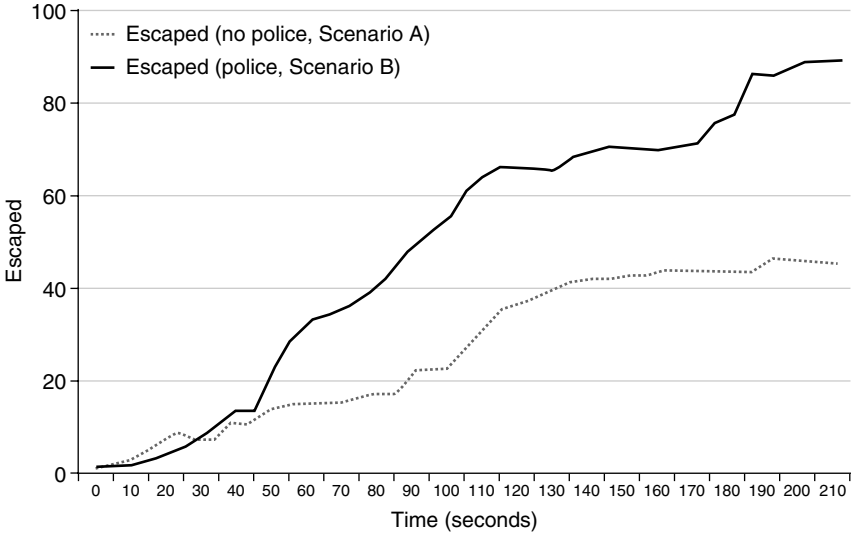


(a)



(b)

Figure 11.6 Simulations of the Westgate Shopping Mall attack: (a) Scenario A (without security officers); (b) Scenario B (with security officers); (c) numbers of escapees over time in Scenario A and Scenario B.



(c)

Figure 11.6 Continued

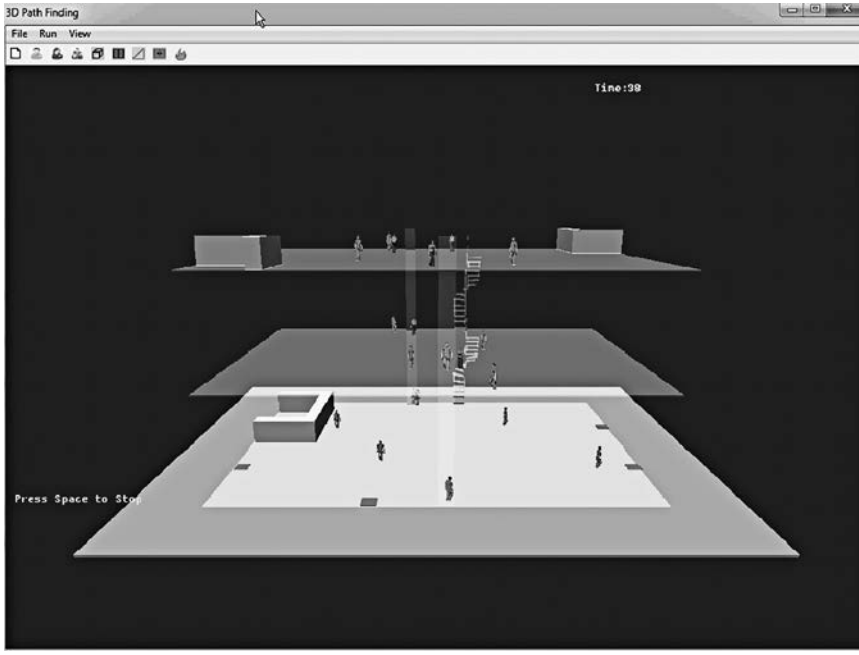
Emergency response plans for escaping from high-rise buildings

As terrorists and violent extremists attack vulnerable and innocent people seemingly at random, it is important to address how communities and individuals handle these traumatic situations, particularly with regard to to vulnerable populations such as the elderly, children and disabled individuals (Hans and Mohanty, 2006). However, in the current emergency preparedness and response systems, those populations, largely the elderly and the disabled, are overlooked (Williams, 2007). It has become clear that emergency plans in their current state on the federal and local level are insufficient and rarely can cope with special cases such as frail elderly, handicapped or medically dependent individuals (Gatty, 2009). This is the first indicator that emergency response teams and disaster plans need to adjust their protocols to better support those populations to quicken recovery, lessen emotional trauma and save the lives of citizens. Escaping from high-rise buildings is particularly challenging for elderly people and people with disabilities.

Since the terrorist attack on the World Trade Center on 11 September 2001, counter-terrorism and response now need to prepare for other terrorist attacks on high-rise buildings (skyscrapers). According to the World Trade Center evacuation study (Gershon *et al*., 2007; Gershon *et al*., 2012), one of the factors that affected evacuation was preparedness planning. Thus the effect of fire drills was explored in the following experimental scenario (Scenario C; see Figure 11.7a).

The extension of the GENIUS framework provides an ability to construct multiple-story high-rise buildings and place stairs (fire escapes) and elevators at any location of each floor. Exits can be located on the ground floor. Different kinds of agents can be placed on each floor and a scheduled event (fire or gas) can be set on any spot of the floor.

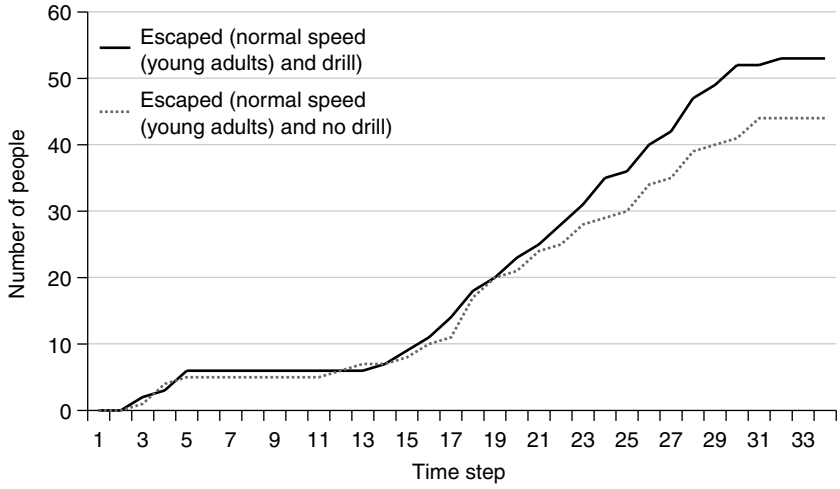
In the experiments, a 10-story building was used and six people were placed on each floor. The scheduled fire was set on the tenth floor. The same number of stairs, elevators and exits with the same locations were used for each experiment. Two different age groups were tested: young adults versus older adults. Older adults had more physical limitations than young adults in terms of walking speed and sight distance. For each age group, two experiments were conducted: one with the agents who had had fire drills and the other with the agents who had had no fire drills. Those who had had fire drills could find stairs and exits more quickly than those who had not.



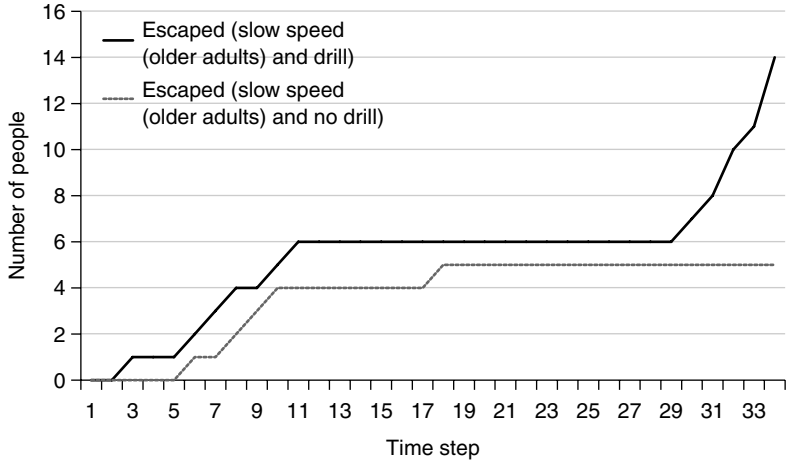
(a)

Figure 11.7 Initial setup and plots of a typical run in Scenario C: (a) the setup of Scenario C, (b) the number of escapees of young adults over time in Scenario C (drills vs. no drills), (c) the number of escapees of older adults over time in Scenario C (drills vs. no drills), (d) the number of escapees of both young and older adults over time in Scenario C (drills), (e) the number of escapees of both young and older adults over time in Scenario C (no drills) (from Park *et al*., 2012).

Figure 11.7b shows the difference between previous fire drill experience and no experience for young adults. After 34 cycles, about 88 percent of the young adults who had had fire drills escaped from the building, whereas 73 percent of those who had not had fire drills escaped. The difference is much bigger for the case of older adults (Figure 11.7c): 23 percent of the older adults who had had fire drills escaped after 34 cycles whereas only 8 percent of those who had not had fire drills escaped. Figure 11.7d and Figure 11.7e show the difference between young adults and older adults for both cases of fire drills and no fire drills, which is about 65 percent. It is observed that a fire drill exercise helps people find fire stairs and escape quickly.



(b)



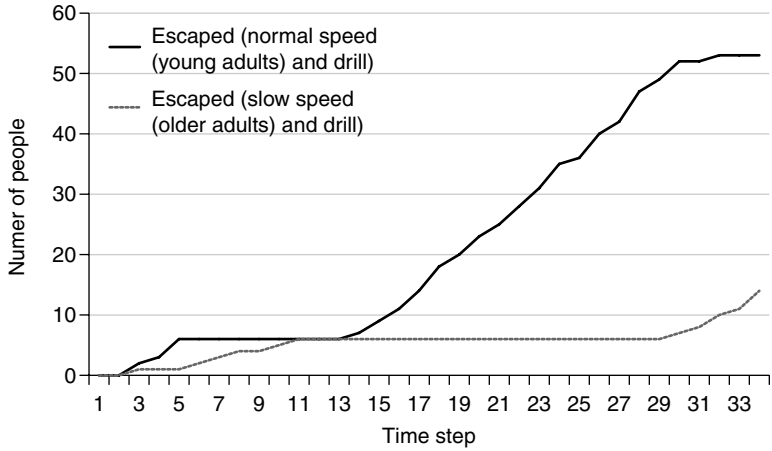
(c)

Figure 11.7 Continued

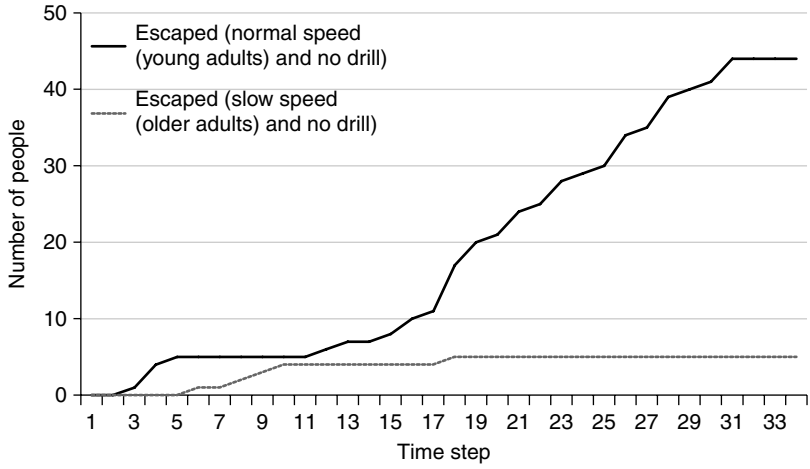
The difference between young adults and older adults in escaping from high-rise buildings is relatively large. This suggests that people who have physical limitations need better ways of escaping from high-rise buildings.

Virtual environments as a training tool for first emergency responders

After creating and verifying optimal and relevant emergency response plans and protocols with the GENIUS system, it is important to prepare and train first emergency responders with those plans and protocols. However, setting up physical environments for such training is often very costly and they are not



(d)



(e)

Figure 11.7 Continued

necessarily reusable. A virtual environment can be a good alternative to a physical one for training purposes. As mentioned above, virtual environment technologies have become affordable, portable, and easy to use. Realistic and immersive virtual environments can be created in a relatively short time. Another benefit is that they can be easily modified. They can be more immersive and realistic with surrounding sound and other sensor devices (such as haptic devices). Literature shows that these virtual environments have been used to train first emergency responders (Vincent *et al*., 2008; Wilkerson *et al*., 2008; Andreatta *et al*., 2010).

In our study, a training program for first emergency responders was developed utilizing currently available technologies. An immersive virtual environment was created using a big-screen projection. For participants' natural interactions with the virtual environment, a gesture and motion-based interaction was developed using a Microsoft Kinect device. The immersive virtual environment was tested with over 20 students. After learning how to navigate the virtual environment with their walking motion and different gestures in the practice session, they all successfully navigated the environment to reach the destination. A few more tests have been done to see how the user can interact with virtual agents. This user's interaction with the immersive virtual environment and virtual agents from the first person's view is important in training because it creates presence: users feel that they are in the environment. Currently we are developing a feature in which the user can lead civilian virtual agents in a certain direction or to an exit, and we are planning to conduct an extensive usability test with police officers in the near future. Figure 11.8 shows our current setup where the user interacts with the virtual environment.

Conclusion and future research

Nobody and no places are immune to terrorism by violent extremists who are well supported globally by like-minded people, either religiously or politically. Our neighbors can be radicalized and recruited online by terrorists through social media (Thompson, 2011). It is our first priority to detect terrorist threats and prevent them from occurring in the first place. However, when a terrorist attack occurs despite our best efforts, a rapid emergency response should be carried out with well-planned protocols. As Perry and Lindell (2003a) mentioned, this can be possible when there are well-established plans, continuous training, and well-updated written protocols.

This chapter has presented a series of studies to develop a computational framework for counter-terrorism and public safety. The outcome of this framework is the GENIUS system. The GENIUS system can provide aid to emergency management authorities in their emergency planning process. The structure of the system is based on multi-agent and parametric modeling. This enables the user of the system to customize agents with different characteristics such as age, gender and personality for creating different actors (police, civilian and terrorist). The system also allows the user to create environments where different scenarios

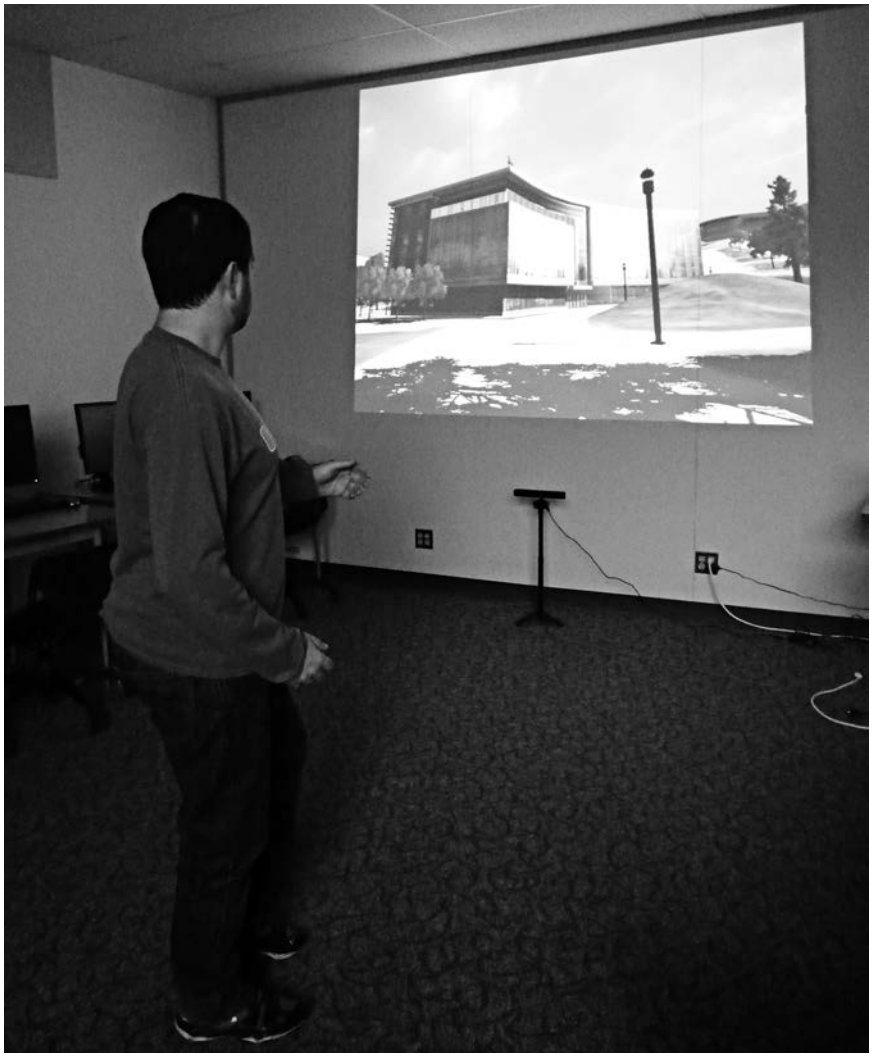


Figure 11.8 The current setup of GENIUS; the user is interacting with the virtual environment using the Microsoft Kinect device (photo by Andrew Park).

can be simulated with agents. We have described a series of simulation experiments using the GENIUS system. Many simulations were based on real terrorist attacks that had happened in the recent past, while the other simulations were based on hypothetical scenarios. The results show that the rate of rescuing people was increased by placing first emergency responders at strategic locations. This demonstrates the customizability, applicability and usability of the GENIUS system.

Another application of the GENIUS system is to train first emergency responders. In addition to running simulation systems, the GENIUS system allows the setup of an immersive virtual environment where the user can navigate and interact with agents in the first person's view. With realistic scenarios, the user can learn and practice emergency plans and protocols.

Although our framework was based on prior literature and our own previous studies of human behaviors, it has a few limitations. One such limitation is that it has not extensively been tested against real cases with experts and/or practitioners. This is necessary to make the GENIUS system practically useful for emergency planning practitioners and first emergency responders. Another limitation of the current study is that agents' behaviors sometimes seem too simple to be used for training purposes. In order to simulate thousands of agents simultaneously, agents cannot be too complicated due to computational limitations. However, we need to find the right balance between agents' natural and realistic behaviors and computational resources.

The GENIUS system is currently being ported to an advanced graphics (game) engine (Unity 3D) to extend its features and accommodate more realistic/complex emergency planning. This enhanced version of the GENIUS system will also have a new feature of simulating police officers' control of a violent and emotionally charged crowd such as the Vancouver Stanley Cup riots in 2011. In order to add more realism and immersion to virtual environments, a new stereoscopic virtual reality goggle (Oculus Rift) will be used. Furthermore, we are planning rigorous usability tests with practitioners.

Acknowledgments

The authors appreciate the input and helpful discussions from members of the Applied Research Lab at Trinity Western University (TWU) and the generous support from the Institute for Canadian Urban Research Studies (ICURS). This project was supported in part by a grant from the Canadian Network for Research on Terrorism, Security and Society (TSAS). The authors acknowledge all the efforts of two research assistants, Andrew K. Park Jr. from the University of Waterloo and Alex Touchet from the Thompson Rivers University, who programmed the GENIUS system. The authors would also like to thank the IRMACS Centre at Simon Fraser University for providing a collaborative and interdisciplinary research environment.

References

Andreatta, P. B., Maslowski, E., Petty, S., Shim, W., Marsh, M., Hall, T., Stern, S. and Frankel, J. (2010) Virtual reality triage training provides a viable solution for disaster-preparedness. *Academic Emergency Medicine*. 17 (8), pp. 870–876.

Beni, G. and Wang, J. (1989) Swarm intelligence in cellular robotic systems. *Robots and Biological Systems: Towards a New Bionics?* Berlin and Heidelberg: Springer, pp. 703–712.

Bonabeau, E. (2002) Agent-based modeling: Methods and techniques for simulating human systems. *Proceedings of the National Academy of Sciences of the United States of America 99* (Suppl. 3), pp. 7280–7287.

Brooks, B. E. (2010) Law enforcement's role in US counterterrorism strategy. *The Police Journal.* 83 (2), pp. 113–125.

Eberhart, R. C. and Hu, X. (1999) Human tremor analysis using particle swarm optimization. In *Evolutionary Computation, 1999. CEC 99. Proceedings of the 1999 Congress on Evolutionary Computation (Vol. 3)*, IEEE. pp. 1927–1930.

Forsyth, D. (2010) *Group Dynamics*. Cengage Learning.

Gatty, B. (2009) Frontlines view on Washington disaster planning for elderly "woefully inadequate." *Long-Term Living.* 58 (8), p. 14.

Gershon, R. R., Magda, L. A., Riley, H. E. and Sherman, M. F. (2012) The World Trade Center evacuation study: Factors associated with initiation and length of time for evacuation. *Fire and Materials.* 36 (5–6), pp. 481–500.

Gershon, R. R., Qureshi, K. A., Rubin, M. S. and Raveis, V. H. (2007) Factors associated with high-rise evacuation: qualitative results from the World Trade Center evacuation study. *Prehospital and Disaster Medicine*. 22 (3), pp. 165–173.

Gilbert, N. (2008) *Agent-Based Models*. Thousand Oaks CA: Sage.

Hans, A. and Mohanty, R. (2006) Disasters, disability and technology. *Development*. 49 (4), pp. 119–122.

Hanyu, K. (1997) Visual properties and affective appraisals in residential areas after dark. *Journal of Environmental Psychology*. 17 (4), pp. 301–315.

Hanyu, K. (2000) Visual properties and affective appraisals in residential areas in daylight. *Journal of Environmental Psychology*. 20 (3), pp. 273–284.

Herzog, T. R. and Flynn-Smith, J. A. (2001) Preference and perceived danger as a function of the perceived curvature, length, and width of urban alleys. *Environment and Behavior*. 33 (5), pp. 653–666.

Izquierdo, J., Montalvo, I., Pérez, R. and Fuertes, V. S. (2009) Forecasting pedestrian evacuation times by using swarm intelligence. *Physica A: Statistical Mechanics and its Applications*. 388 (7), pp. 1213–1220.

Kennedy, J. and Eberhart, R. (1995). Particle swarm optimization. *IEEE International of first Conference on Neural Networks*.

LaGrange, R. L., Ferraro, K. F. and Supancic, M. (1992) Perceived risk and fear of crime: Role of social and physical incivilities. *Journal of Research in Crime and Delinquency*. 29 (3), pp. 311–334.

Onuoha, F. C. (2013) Westgate attack: Al-Shabab's renewed transnational jihadism. *Al-Jazeera Center for Studies*, 11 November.

Park, A. J., Hwang, E., Spicer, V., Cheng, C., Brantingham, P. L. and Sixsmith, A. (2011) Testing elderly people's fear of crime using a virtual environment. Paper presented at Intelligence and Security Informatics Conference (EISIC), 2011, IEEE, pp. 63–39.

Park, A. J., Spicer, V., Guterres, M., Brantingham, P. L. and Jenion, G. (2010) Testing perception of crime in a virtual environment. Paper presented at Intelligence and Security Informatics (ISI) 2010 International Conference, IEEE, pp. 7–12.

Park, A. J., Tsang, H. H., Sun, M. and Glässer, U. (2012) An agent-based model and computational framework for counter-terrorism and public safety based on swarm intelligence. *Security Informatics*. 1 (1), pp. 1–9.

Pelechano, N. and Badler, N. I. (2006) Modeling crowd and trained leader behavior during building evacuation. *IEEE Computer Graphics and Applications.* 26 (6), pp. 80–86.

Perry, R. W. and Lindell, M. K. (2003a) Preparedness for emergency response: guidelines for the emergency planning process. *Disasters*. 27 (4), pp. 336–350.

Perry, R. W. and Lindell, M. K. (2003b) Understanding citizen response to disasters with implications for terrorism. *Journal of Contingencies and Crisis Management*. 11 (2), pp. 49–60.

Primakov, E. M. A. (ed.) (2004) *World Challenged: Fighting Terrorism in the Twenty-First Century*. Brookings Institution Press.

Sampson, R. J. and Raudenbush, S. W. (1999) Systematic social observation of public spaces: A new look at disorder in urban neighborhoods 1. *American Journal of Sociology*. 105 (3), pp. 603–651.

Schmid, A. P. (2012) The revised academic consensus definition of terrorism. *Perspectives on Terrorism*. 6 (2), pp. 158–159.

Thompson, R. L. (2011) Radicalization and the use of social media. *Journal of Strategic Security*. 4 (4), pp. 167–190.

Tsang, H. H., Park, A. J., Sun, M. and Glasser, U. (2010) GENIUS: A computational modeling framework for counter-terrorism planning and response. Paper presented at Intelligence and Security Informatics (ISI), 2010 IEEE International Conference, IEEE, pp. 71–76.

Vincent, D. S., Sherstyuk, A., Burgess, L. and Connolly, K. K. (2008) Teaching mass casualty triage skills using immersive three-dimensional virtual reality. *Academic Emergency Medicine*. 15 (11), pp. 1160–1165.

Wakita, T., Ozawa, K., Miyajima, C. and Takeda, K. (2005) Parametric versus non-parametric models of driving behavior signals for driver identification. In Kanade, T., Jain, A. and Ratha, N. K. (eds) *Audio-and Video-Based Biometric Person Authentication*. Berlin, Heidelberg, New York: Springer, pp. 739–747.

Walls, R. M. and Zinner, M. J. (2013) The Boston marathon response: why did it work so well? *Journal of the American Medical Association*. 309 (23), pp. 2441–2442.

Weinrath, M., Clarke, K. and Forde, D. R. (2007) Trends in fear of crime in a western Canadian city: 1984, 1994, and 2004. *Canadian Journal of Criminology and Criminal Justice/La Revue canadienne de criminologie et de justice pénale*. 49 (5), pp. 617–646.

Wilkerson, W., Avstreih, D., Gruppen, L., Beier, K. P. and Woolliscroft, J. (2008) Using immersive simulation for training first responders for mass casualty incidents. *Academic Emergency Medicine*. 15 (11), pp. 1152–1159.

Williams, M. M. (2007) Invisible, unequal, and forgotten: Health disparities in the elderly. *Notre Dame Journal of Law, Ethics and Public Policy*. 21, pp. 441–478.

12 Radical and connected

Concluding thoughts and future research

Martin Bouchard and Evan Thomas[1]

When Micheal Zehaf-Bibeau entered the Ottawa Parliament in Canada on 22 October 2014 and shot Corporal Nathan Cirillo before being fatally wounded himself, many questions arose, with two of them being of particular interest to us in the context of this book. First, is it a *terrorist* incident, or a *criminal* incident involving an individual with mental health issues? Second, why now—or why did the incident happen on October 22 and not on any other date?

The first question inquires about the nature of the incident and the label to attach to it. The label matters because it has implications for understanding what happened and, perhaps most importantly, designing a suitable policy treatment to it. The *terrorism* label leads to a distinct set of policy recommendations which focus on individuals who radicalize, the role of the Internet in radicalization, and on Zehaf-Bibeau's conversion to Islam many years prior as an important piece of the puzzle. This view is subject to taking this case of lone actor terrorism and generalizing it to a broad set of counter-terrorism policies. The *criminal/mental health* label focuses on the prior documented criminal behavior of the offender and leads to a standard criminal justice response as it would to any public shooting incident. The focus is then not on terrorism but on the immediate individual factors that may have precipitated this type of hard-to-predict, extraordinary incident (see Huey in this volume). This view, for better or for worse, does not impact the counter-terrorism policies in Canada. No matter which camp one chooses,[2] the one common implication is that both reactions call for increased security around Parliament to prevent a potential shooter from entering the premises unchecked.

The Royal Canadian Mounted Police (RCMP) quickly answered the first question with a yes: the RCMP Commissioner reported that Zehaf-Bibeau had prepared a video discussing the incident he was planning where his political and ideological motives were made clear (MacCharles, 2014). Yet his mother was among others who expressed doubts that he truly had ideological motives, pointing out his history of mental illness and drug use. As journalist Allan Woods (2014) reported, the criminal label camp includes Muhammad Robert Heft, well-known activist involved in the de-radicalization of young Muslims, who wrote on his Facebook page:

> I found that the biggest losers in society were the perfect so-called jihadists because they already have criminal behavior, hate authority and have no respect for society.… They never submitted to Islam but took the most controversial parts of it and exploited them for their own personal gain.
>
> (Woods, 2014)

Perhaps this is a false dichotomy, and the reality is much greyer. In fact, all of these elements point toward Zehaf-Bibeau fitting the usual profile of the lone wolf terrorist. McCauley and Moskalenko (2014) recently reviewed the literature on lone wolf terrorists and found four common characteristics associated with many of them: they are motivated by a personal grievance, they suffer from depression or another mental disorder, they have a history of weapon use outside of the military, and they have undergone a situational crisis of personal disconnection and maladjustment that precipitated their violent act. Yet their research also shows that these same characteristics were also commonly found in other types of lone actor violent offenders, such as school attackers and adult assassins. To say that Zehaf-Bibeau's incident is clearly terrorism or that it is clearly the extreme outcome of a long-established pattern of criminal behavior may miss the complexity of the trajectory that led him to the Ottawa Parliament on that fateful day.

The second question is more difficult to answer than the first because the answer depends on having access to Zehaf-Bibeau's mental state in the months, weeks, and days leading up to the incident. Yet reflecting on the timing of the incident is useful in shedding light on some aspects of this debate, including some of the themes covered in this volume. Timing matters because the decision to commit a violent offence is often associated with personal precipitating factors in the weeks or days preceding the incident. McCauley (2014) points to such a personal grievance in the Zehaf-Bibeau's case that, combined with the rest of his profile as a loner with a history of mental illness and drug use, produces a compelling case for a specific type of perpetrator where timing is crucial to the story:

> It is important to notice that pointing to Islam as the instigation for his attack is a weak explanation: Zehaf-Bibeau was a practicing Muslim for seven years, how can Islam explain how he suddenly attacked only this week? A more personal grievance is more immediate. Zehaf-Bibeau was applying for a passport to visit either Syria (according to his mother) or Libya (according to an acquaintance at the Ottawa Homeless Shelter). He was being held up as Canadian authorities weigh concerns about whether he might go to Syria to fight with Islamic State. This personal grievance, this personal frustration, appears to be the immediate precursor of his attack.

Another precipitating factor could have been less personal but is perhaps just as important in explaining the timing of Zehaf-Bibeau's actions: the incident involving radicalized Muslim convert Martin Couture-Rouleau, who had also

killed a member of the Canadian military only two days earlier and less than 150 miles away. While Zehaf-Bibeau may have been thinking about his actions for a long time prior to Couture-Rouleau's incident on October 20 (and thus this does not constitute a pure form of "imitation"), the decision to act immediately after points to the Couture-Rouleau incident as the last push Zehaf-Bibeau may have needed to execute his plans.

Timing matters, according to McCauley (2014), because it decreases the importance placed on religion in trying to explain a specific incident. The arguments for the decreased importance of religion in radicalization usually point out to another set of factors—notably those involving social networks and group cohesion—in differentiating between radicals who act and those who do not. Yet we see no contradiction in accepting that both religion and social networks matter in perhaps a majority of cases. Social networks, of course, matter less for lone wolf actors (McCauley and Moskalenko, 2014)—at least the offline, face-to-face interactions that many point out as crucial in radicals becoming terrorists (McCauley and Moskalenko, 2008; Sageman, 2004, 2008). Because the online life of lone actor terrorists is often filled with a wide-ranging virtual network of individuals sharing their views and interacting with these actors for years and months before they act out, one might consider the possibility of the Internet playing a key role in the process of radicalization when addressing lone wolves in particular.

Understanding the timing of an incident is important in thinking about prevention as well. If it is the case that Zehaf-Bibeau's incident can be associated with precursors such as the interdiction to travel abroad, then increased attention should be given to the surveillance individuals whose passport requests have been denied. Similarly, if imitation is a factor to explain the timing of some violent incidents, then authorities should be increasingly vigilant—and perhaps invest additional resources—in the surveillance of high-risk offenders in the days and weeks following a high-profile incident. As always, it is important that any surveillance and intervention by authorities be framed within the limits allowed by the criminal justice system. In the aftermath of the two October 2014 events in Canada, the risks of abuses and over-targeting are as high as ever.

Ten contributions from this book

A useful way to summarize the contributions of this volume is to derive 10 statements, one for each chapter, capturing the main idea presented by the authors. We connect the findings presented in each chapter to this main idea and also reflect on possible extensions to future work in that area.

1 Some of the causes of modern terrorism are deeply rooted in history

This is the message to be taken from Gerolymatos' (Chapter 2, this volume) detailed account of the history of modern terrorism in the Middle East. The roots

of Middle Eastern terrorism can be understood by analyzing turning points in the way society was organized and governed and the involvement of outside states. Armed insurgencies and the transition of ruling authority fit into a broader historical narrative. We can see with a historical perspective that terrorism is not merely a contemporary phenomenon and should not be treated as such. Rather, it is rooted in a string of violent actions and reactions by both Western and domestic forces shaping the mode of conflict. The rise of the Muslim Brotherhood, the defeat of the Palestinians in 1936, the movement towards Arab unity each developed a theme for successive generations, and the idea of Muslim oppression is being capitalized on by contemporary extreme and violent radicals. The oppression of the broader Muslim community is one of the key factors motivating those who travel to conflict zones. As Gerolymatos points out, the interconnected narratives dovetail into one another. The Islamic State has attracted followers internationally through extensive exploitation of the narratives propagated by Al-Qaeda, indoctrinating recruits in their version of misappropriated Islam. Its use of terror as a "spear" is the evolution of the ongoing development of conflict. As violent extremists assume these narratives online and are persuaded by them, examination of the way the discourse connects those at risk is necessary.

2 Outliers should not be discarded as undesirable

As argued by Huey and colleagues (Chapter 3, this volume), over-reaching what the empirical data implies is dangerous and limits the validity of conclusions that follow. If our case studies are inappropriately grouped, how can we be sure of policies modeled on them? Multi-platform data sources, the reuse of datasets, unsystematic drawing upon academic accounts, and inferences through analogy all pose methodological risks. From this perspective, Huey *et al.* make explicit recommendations for future research that are worth reiterating here: (1) respect the levels of analyses, (2) draw systematically from other bodies of work, and (3) focus on the production of novel research.

3 Network concepts and methods are powerful tools to move the field forward

There is a long list of social and natural phenomena that have been better understood from adopting a network approach (Borgatti *et al*., 2009; Watts, 2004), and terrorism is one of the newest fields to witness an upsurge in research on networks (Bouchard and Nash, Chapter 4, this volume). Networks are democratic—they can be used to more precisely describe the organization of terrorist groups, but they can be just as useful in describing the structure of the agencies and task forces that combat terrorist activity. Networks can be used as predictors of an outcome of interest (e.g., Helfstein and Wright's 2011 analysis of group structure and lethality) or as outcome measures in their own right (e.g., Everton and Cunningham's 2013 analysis of the network effects of various events in

Noordin Top's network). Network analysis can be used for simulating the effects of potential interventions prior to the unleashing of a terrorist act or to evaluate the impact of these interventions once they have occurred. Horgan (2008) emphasizes the "routes" over "roots" paradigm, where mapping the pathways of terrorists can be more informative than seeking causal roots. Networks are powerful because so much of many phenomena can be understood simply by mapping and analyzing the underlying social network.

4 The personal radicalization process is best understood by following the evolution of a person's social network

The social interactions of sympathizers, radicals, and terrorists are just as varied in nature, frequency, and intensity as the interactions of the rest of the population. As shown in Nash and Bouchard's (Chapter 5, this volume) network trajectory analysis of homegrown terrorist Omar Hammami, these interactions change over time, the views of these individuals evolve, and researchers need to systematically collect the social network data of these individuals longitudinally to fully understand what caused the change and when it occurred. Significant network changes were also associated with clear turning points in Hammami's personal radicalization process, thus providing some of the ingredients for prevention and intervention prior to Hammami reaching the final stages of his radicalization. In Hammami's case, the gradual replacement of his pre-radicalization network with a new one made up of almost exclusively jihadi brothers can be observed as he starts traveling around the world to pursue his "personal jihad." Nash and Bouchard also show how his networks of family and friends start to co-exist at one point in his trajectory until the co-existence is no longer tenable.

5 People connecting multi-dimensionally have to be examined multi-dimensionally

Both the chapters by Nash and Bouchard (Chapter 5, this volume) and the one by Ducol (Chapter 6, this volume) remind us to engage our understanding of radicalization primarily in the way people socialize and select behaviors without making premature inferences on the role of Internet in this process. As argued by Ducol, there is a gap in the research literature caused by multiple difficulties including the clandestine nature of the subjects, the bias of the researchers presuming causality, the presumption of a vulcanized online and offline reality on the part of the radicalized, and the lack of a conceptual foundation contextualizing the Internet's facilitation in existing radicalization frameworks.

As people prioritize and rearrange aspects of their life (or spheres) in both frequency and importance, we can expect a change in their "sociability." The tacit argument for analysis by Ducol in this line of thought is that the Internet is over-emphasized in the research literature and a greater role exists for the process of selection of *life-spheres* instead of focusing on how the Internet radicalizes the individual. The causal role of the Internet community, here, is what is

up for debate. Is it that the entirety of someone's behaviors is changing, or is their online presence driving the change? Research undertaken to examine the behaviours of individuals as they develop both online and offline in tandem will fill this void. Analysis that approaches behavior and socialization development across multiples spheres of activity is the next step in evaluating the exact processes the Internet influences.

6 Extremist groups still vary widely in their use of the Internet and social media for recruitment

Davies *et al.* (Chapter 7, this volume) find that extremist groups vary greatly in their use of the Internet for recruitment purposes. Groups appear to make a choice between being providers of information on the group and its cause while using violent, graphic material; or they actively try to recruit new members while remaining mostly non-violent in the content they publish. The groups traditionally labeled as right-wing (e.g., Aryan Nations) and left-wing (e.g., Animal Liberation Front) extremists tend to be the most actively involved in recruitment to their respective causes, while groups that defend a relatively local cause such as FARC or the Popular Front for the Liberation of Palestine use violent material without explicitly (at least with words) attempting to expand their group of followers. The strategies and online presences differ, but the implicit objectives of all of these groups may nonetheless remain relatively similar.

Websites build a narrative, rationalize their goals, and finally, for some groups, provide opportunities to join. The levels of violence and the openness with which they operate all are still specific to the group and its particular limitations (Davies *et al*., Chapter 7). Common, though, is the logic of building support and presence online in order to perpetuate the group. As Conway (2006) describes, the use of social media predominantly revolves around building and maintaining of narratives—and this occurs in phases. Further assessment of the effectiveness of levels of specific messages, the way their narratives unfold and the mechanisms through which users can join the cause will provide new insight into how to prevent such groups from effectively communicating their message to potential recruits.

7 Cyberwarriors are still an unknown variable, and flux in political circumstances can change the pool of potential actors

Holt *et al.* (Chapter 8, this volume) take an important step in showing how survey research can be used by researchers to study scenarios in cyberterrorism. In an original study and research design that should be replicated for comparative purposes, Holt *et al.* described the impact varying political situations and impetus can have on the willingness to engage in cyberattacks (Chapter 8). As political motivation changes, the interest in both domestic and international cyberattacks become more common. Even if, as Holt *et al.* have noted, the study only indicates a purported willingness and not an assured reaction, the increased

pool of potential recruits, in the right context, could have tangible consequences. Holt *et al.* set a launching point for studying key "turning points" in political developments and their impact on online discourse.

8 It does not necessarily take a network to fight a network

Dupont (Chapter 9, this volume) is explicit in the view that all networks are not made equal; government networks, lacking the specificity of purpose, trust and operational freeness (legality) that characterize terrorist networks, are inherently disadvantaged. The new orthodoxies being adopted by governments present new challenges. Among those pertinent to the discussion of anti-terrorism efforts are three paradoxes: those of legality, information and trust. While networks provide a variety of benefits for security agencies, security agencies face considerable new challenges in the process of integrating into the networks Dupont describes, and these challenges require additional management efforts. The process of trading information, in the spirit of collaboration, comes with a host of potential benefits but also a new set of risks that have prevented effective cooperation in the past. For example, information overload risks inundating agencies while preventing valuable information from being analyzed. Moving forward, a careful, systematic examination of the structures of cooperation among law enforcement agencies involved in national security can facilitate the established of best practices in the creation of multi-agency security networks.

9 Integration of institutions is not a panacea

Kitchen and Molnar explicitly state that "integration and collaboration are not a panacea" (Chapter 10, this volume). Such cooperation risks replacing one problem (e.g., ineffective communication and coordination) with another (e.g., inability to come together as a single unit). In Kitchen and Molnar's terms, this may solve a silo problem but leads to new inefficiencies, different complexities, security issues, and a diffusion of legal culpability. The risks of both regulatory arbitrage and information overload need to be presented and weighed against actual, not perceived, gains, and questions still remain about the actual benefits. The benefits that are seen in Shiprider (or possibly NxtGen) are attractive, but as argued by Kitchen and Molnar there remains a significant amount of analysis to be undertaken before definitive statements can be made about its desirability (at the rate it has so far been implemented). The investigations of network approaches put forth in this volume do not mean that such approaches should be applied anywhere, everywhere, without careful consideration of the new challenges emerging.

10 Simulation research can greatly assist emergency preparedness

Maximizing public safety after a terrorist event or natural disaster requires attention to specific factors. Victory favors preparation, and virtual models are

demonstrating the optimal use of resources in multiple emergency scenarios. Written, formal, prepared plans are a necessity, but equally important is well placed and well trained guardianship that can move with efficacy and flexibility. As showed by Park and Tsang (Chapter 10, this volume), computer based modelling can allow both the demonstration and the development of skills by first responders in an emergency context.

The effective integration of technology creates capacity beyond researching greater scope or greater detail—it provides entirely novel avenues of study, predicting group dynamics in an artificial world. The study of reactions and simulated events shows promise as tools are developed with more refined data and real world examples upon which to build the accuracy of the simulation. Although the authors only go so far as to discuss the response to an event, from here, more complicated evaluation of defense strategies and proactive simulations are possible.

Concluding thoughts: elements of a research agenda for terrorism and social networks

Integrate network data collection methods to research and evaluate counter-terrorism operations, especially those involving multiple agencies and jurisdictions

The introduction of social network analysis can help evaluate inter-agency cooperation and collaboration. The social structure underlying the collaborative networks should not be assumed to be a constant—the merging of groups of individuals trained in different agencies may produce a myriad of unique social interactions that may affect the outcome of an investigation. Effective response times, caseloads versus case completions, effective information used or traded can all be tested against network measures. As Bouchard and Nash (Chapter 4) reminded us, any group or organization can be analyzed as a network. Not all hierarchies behave the same, and not all horizontal partnerships are made equal. Network methods allow this variability to be mapped and allow the organizational structure not to be taken for granted. The research design argument we make here is, of course, different from the more general one made by Dupont in chapter 9 on organizational styles. In that alternative view of networks, the term "network" (what we ought to do) is used in opposition to a term such as "hierarchy" (what we do now).

Within the intelligence community, there appears to be an understanding that agencies face inherent limitation due to the legal structures they operate in (Whelan, 2014). The limitations are often ignored because of a perceived failure of hierarchical structures (Dupont, 2006). Managers of security organizations have difficulty managing the balance flow and direction of information and organizational tension. The revealed stress, as well as the demonstrated shortcomings (Kitchen and Molnar, Chapter 10), indicate there is room for greater efficiency and focus—all of which can be facilitated by proper attention to the development of trust networks.

Using network measures, agencies can be analyzed to evaluate where organizations overlap and to evaluate the optimal density of connections. When evaluating the properties of networked agencies using a network perspective, researchers can think of the optimization of efficient cooperation without degrading the structure of the existing hierarchies to which the actors belong.

Reflect on the options for using the Internet for interventions to counter violence and extremism

As is alluded to by Neumann (2013), engaging in Internet usage for the purposes of communication, propaganda, fund-raising, radicalization, and recruitment seems to be a numbers game more than anything else. The more people you can reach with an influx of information, the higher the likelihood of radicalization with the maximum number of individuals possible. Thinking about the implications of this exposure argument for countering violent extremism, there are two questions of interest. First, is it a good idea to try to restrict the extremist content online so as to try to reduce exposure? Second, can the power of the Internet be used for de-radicalizing youth, that is, using the exposure model for pro-social benefits?

With regard to the first question, scholars disagree with the notion of restricting online access to certain extremist sites, due to both a hesitation to limit civil liberties and the practical difficulties (Neumann, 2013; Torres-Soriano, 2012). Soriano (2012) underscores the impracticality of attempting to eradicate all extremist web sources, as these online sites could simply be reproduced as quickly as they were taken down. The elimination of all jihadist and extremist web sites "would require tasking the same number of people to attacking the sites as the number willing to set up new ones" (Soriano, 2012, p. 268). However, the task of continually and repetitiously targeting certain main jihadist websites promoting violence and radicalization has proven to be fairly effective, and should carry on as a means of deterring future websites (Soriano, 2012).

The answer to the second question is a definitive "yes." First, user-generated online content can be of benefit to intelligence agencies directly (Neumannm 2013; Ryan, 2007). There is utility and, in fact, advantage in social media being used to engage content creators and not censor them (Ryan, 2007). Many studies focus on the development of online discourse, but capitalizing on the discourse can also utilize the political and cultural elements that impact the development of extremism (Gerolymatos, Chapter 2, this volume). Battling for the "hearts and minds" is visible strategy of foreign policy (Aldrich, 2014), but the transition to the digital sphere is still developing. Neumann (2013) stresses the importance of "creating awareness" among the community, especially those holding positions of authority, in the hopes that these individuals will detect and report on behavioral/attitudinal signs of radicalization.

The benefits associated with use of the Internet are undisputed, but the inherent vulnerabilities associated with it are not always expanded upon despite great potential (Ryan, 2007; Soriano, 2012). The idea of anonymity is not as ubiquitous as it may initially seem (Soriano, 2012). Thus this assumed advantage of

free and open speech has what Soriano (2012) calls a "flip-side" to it. Online extremists and terrorists may have the ability to disseminate information at a rapid rate, and to far ends of the world, but counter-intelligence agencies have the ability to intervene and debilitate such communications. The web allows for individual users to ridicule and question violent and extremist materials, even within networks (or forums) of already seemingly radicalized individuals (Soriano, 2012). As Soriano (2012) put it, "the more *Jihadist* terrorism commits to Web 2.0 the more it exposes its discourse to challenge" (p. 274).

Continue the push to innovate in research on terrorism and global media

Violent radicals are adapting to capitalize on the ease of access that Web 2.0 promises—and researchers are doing the same. Even as extremists exploit interaction and anonymity on the web, it is possible to tap into behavioral patterns, dissemination of ideas, and reception of those same ideas. Bowman-Grieve and Conway (2012) discuss the digital footprint of dissidents to explore the role of the Internet for the IRA, and test assertions by the media of their support base (or lack thereof). Bowman-Grieve and Conway (2012) argue that the Internet provides an "always on" (p. 72) space, which plays a pivotal support role in education and production. By analyzing web-forum metrics such as members, growth and maximum users online, the authors begin to evaluate claims about interest and topicality.

The push for innovations includes taking full advantage of the technology while keeping the research questions meaningful for social scientists and policy-makers. Dark web analyses (Zhou *et al*., 2006; Chen *et al*., 2008) have utilized automated software to capture large swathes of user content. Similarly, Bouchard *et al.* (2014) found that an automated data collection process capitalizing on keywords could generate novel approach vectors that allowed for large-scale analysis and description of web site behaviors. Assuming that validity tests confirm the utility of such software, technological innovations in the automation of content analyses are promising, allowing researchers to tackle a large amount of material at the same time. Bermingham *et al.* (2009) capitalized on the methodology and introduced the use of sentiment in contemporary analysis. By evaluating not only the post and the connections the post entails but also the sentiment of posts, the authors could begin to make assertions about the impact of user variables on attitudes. In this particular study, Bermingham *et al.* (2009) found that gender differences related to a more extreme ideology (particularly as it related to the thematic category of *Israel* and *Judaism*).

Embracing the online aspect of empirical research also implies new units of analyses, such as "extremist websites" (Bouchard *et al*., 2014; Burris *et al*., 2000; Davies *et al*., this volume). Ducol (2012), for instance, explicated the French "jihadisphere" and its use of the Internet as a media outlet to connect to global audiences. In his exploratory paper, Ducol (2012) extracted URLs from a seed website to begin his snowball sample and created a virtual network to

examine the extent to which French-speaking jihadi websites were connected. Of particular interest was the analysis of the different approach vectors to particular forums—despite the importance of social bonds in the acquisition of members (41 percent of registrants), the majority came through online bridges (51 percent). Burris *et al.* (2000) had previously evaluated the interconnectedness of right-wing extremists online, focusing on the identification of sub-groups in evaluating centrality and connections.

A particularly important development is the examination of a single organization or ideology but on multiple social media platforms. O'Callaghan *et al.* (2013) incorporated the more dynamic portion of new social media, and extrapolated the focus of Bowman-Grieve and Conway (2012) on online space to the extension into multiple platforms online—the growing interconnectedness of online networks across not only sites but platform *types*. By mapping the interconnection of social media outlets, O'Callaghan *et al.* (2013) were able to test not only for the presence of communities (Bowman-Grieve and Conway, 2012) or the interconnectedness of their websites (Burris *et al*., 2000; Ducol, 2012) but also for *dynamic persistent communities* evident across platforms, and connecting what otherwise might have been studied as separate and isolated networks.

Notes

1 The authors would like to thank Philippa Levey for her assistance in the preparation of this chapter.

2 The leader of the National Democratic Party (the official opposition), Thomas Mulcair, labeled the incident as "criminal behavior" while the leaders of the other two major parties, including Prime Minister Harper, labeled the incident as "terrorist" (Smith, 2014).

References

Aldrich, D. P. (2014) First steps towards hearts and minds? USAID's countering violent extremism policies in Africa. *Terrorism and Political Violence*. 26 (3), pp. 523–546.

Bermingham, A., Conway, M., McInerney, L., O'Hare, N. and Smeaton, A. F. (2009) Combining social network analysis and sentiment analysis to explore the potential for online radicalisation. Paper presented at Social Network Analysis and Mining, 2009. ASONAM'09. International Conference on Advances in Social Network Analysis and Mining, IEEE.

Borgatti, S. P., Mehra, A., Brass, D. J. and Labianca, G. (2009) Network analysis in the social sciences. *Science*. 323 (5916), pp. 892–895.

Bouchard, M., Joffres, K. and Frank, R. (2014) Preliminary analytical considerations in designing a terrorism and extremism online network extractor. In Mago, V. and Dabbaghian, V. (eds) *Computational Models of Complex Systems*. New York: Springer, pp. 171–184.

Bowman-Grieve, L. and Conway, M. (2012) Exploring the form and function of dissident Irish republican online discourses. *Media, War and Conflict*. 5 (1), pp. 71–85.

Burris, V., Smith, E. and Strahm, A. (2000) White supremacist networks on the Internet. *Sociological Focus*. 33 (2), pp. 215–235.

Chen, H., Chung, W., Qin, J., Reid, E., Sageman, M. and Weimann, G. (2008) Uncovering the dark web: A case study of Jihad on the web. *Journal of the American Society for Information Science and Technology*. 59 (8), pp. 1347–1359.

Conway, M. (2006) Terrorism and the internet: New media, new threat? *Parliamentary Affairs*. 59 (2), pp. 283–298.

Ducol, B. (2012) Uncovering the French-speaking jihadisphere: An exploratory analysis. *Media, War and Conflict*. 5 (1), pp. 51–70.

Dupont, B. (2006) Delivering security through networks: Surveying the relational landscape of security managers in an urban setting. *Crime, Law and Social Change*. 45 (3), pp. 165–184.

Everton, S. F. and Cunningham, D. (2013) Detecting significant changes in dark networks. *Behavioral Sciences of Terrorism and Political Aggression.* 5 (2), pp. 94–114.

Helfstein, S. and Wright, D. (2011) Covert or convenient? Evolution of terror attack networks. *Journal of Conflict Resolution*. 55 (5), pp. 785–813.

Horgan, J. (2008) From profiles to pathways and roots to routes: Perspectives from psychology on radicalization into terrorism. *Annals of the American Academy of Political and Social Science*. 618 (1), pp. 80–94.

MacCharles, T. (2014) RCMP calls parliament shootings a "terrorist" attack driven by ideology. *The Star*. 26 October.

McCauley, C. (2014) Ottawa Parliament shooter Michael Zehaf-Bibeau: Ottawa shooter fits the disordered/disconnected profile of lone-actor violence. Available at: www.psychologytoday.com/blog/friction/201410/ottawa-parliament-shooter-michael-zehaf-bibeau. Accessed 29 October 2014.

McCauley, C. and Moskalenko, S. (2008) Mechanisms of political radicalization: Pathways toward terrorism. *Terrorism and Political Violence*. 20 (3), pp. 415–433.

Moskalenko, S. and McCauley, C. (2014) Ottawa parliament shooter Michael Zehaf-Bibeau. *Psychology Today*. 23 October.

Neumann, P. (2013) The trouble with radicalisation. *International Affairs*. 89 (4), pp. 873–893.

O'Callaghan, D., Greene, D., Conway, M., Carthy, J. and Cunningham, P. (2013) An analysis of interactions within and between extreme right communities in social media. In Atzmueller, M., Chin, A., Helic, D. and Hotho, A. (eds) *Ubiquitous Social Media Analysis*. London: Springer, pp. 88–107.

Ryan, J. (2007) The four P-words of militant Islamist radicalization and recruitment: Persecution, precedent, piety, and perseverance. *Studies in Conflict and Terrorism*. 30 (11), pp. 985–1011.

Sageman, M. (2004). *Understanding Terror Networks*. Philadelphia: University of Pennsylvania Press.

Sageman, M. (2008). *Leaderless Jihad: Terror Networks in the 21st Century*. Philadelphia: University of Pennsylvania Press.

Schanzer, D. H. (2014) No easy day: Government roadblocks and the unsolvable problem of political violence—A response to Marc Sageman's "The stagnation in terrorism research." *Terrorism and Political Violence*. 26 (4), pp. 596–600.

Smith, J. (2014) Ottawa shooting not terrorism, say Thomas Muclair. *The Star.* 29 October.

Torres-Soriano, M. R. (2012). The vulnerabilities of online terrorism. *Studies in Conflict and Terrorism*. 35 (4), pp. 263–277.

Torres-Soriano, M. R. (2013) The dynamics of the creation, evolution, and disappearance of terrorist Internet forums. *International Journal of Conflict and Violence*. 7 (1), pp. 164–178.

Watts, D. J. (2004) *Six Degrees: The Science of a Connected Age*. New York: W. W. Norton and Company.

Whelan, C. (2014). Managing dynamic security networks: Towards the strategic managing of cooperation, coordination and collaboration. *Security Journal*. Doi:10.1057/sj.2014.20.

Woods, A. (2014) How Martin Couturer-Rouleau became an aspiring Islamic State fighter. *The Star*. 26 October.

Zhou, Y., Qin, J., Lai, G. and Chen, H. (2007) Collection of US extremist online forums: A web mining approach. Paper presented at System Sciences, 2007, HICSS 2007, 40th Annual Hawaii International Conference on System Sciences, IEEE.

Index

Page numbers in *italics* denote tables, those in **bold** denote figures.

9/11 4, 49, 52, 107, 157, 159, 162, 176; American Commission Report 175; Commission 160; failures of security services 170; homegrown terrorism 51; legislation 169; lessons 191; plans undetected 164; terrorism-related legislation 124; terrorist attacks 36, 38, 56, 128, 156, 168, 187, 196; terrorists 170n1; *see also* post 9/11

Aburish, S.K. 22–3, 30n31
adolescents 108–9, 113
Al-Qaeda 11, 16, 28, 51, 56–7, 110, 112–13, 221; command center 53; digital tools 85; linked to 37; members executed 158; ties 34, 61, 64, 170n1, 206; use of the Internet 107
Al-Rizzo, H.M. 129
Al-Shabaab (Harakat Al-Shabaab al-Mujahideen) 67, 75–6, 206–7; Hammami 61, 64–8, **69**, 70–1, 74, 77; militant ideologies 70; network 78; recruiter 79n3
American 190, 192; 9/11 Commission Report 175; airplanes hijacked 38–9; artist 156; cities 164; citizens 161; Committee for Liberation 24; communications intercepted 163; database 168; diplomats 31n37; documents 20; Embassy 26; homegrown terrorists 34, 61, 64; imperialism 26–7; intelligence agency 22; invasion 27; jihaadi 66; policy after 9/11 12; relationship with Nasser 23–4; representatives 185; strategists 14, 19; terrorism-related deaths 187; *see also* Americans, United States
Americans 16, 19, 26–8; Nasser relationship 23–4; Nazi links 20, 30n16
Andress, J. 129, 131
Anglo-American intelligence officers 16; organizations 13
Animal Liberation Front (ALF) 114, 117, *118*, 119, *120*, **121**, 122–3, *124–5*, 223
Aradau, C. 177, 189
Arkin, W. 158, 162
Arquilla, J. 56, 159
Aryan Nations (AN) 114, *118*, 119, *120*, **121**, 122–3, *124–5*, 223
Asal, V. 49, 56
Associated Press 168
Australia 37; Five Eyes alliance 181; homegrown terrorists 34, 61; national security division 3
Australian 34, 37–8
Awan, A.N. 1–2, 82, 111
Ayatollah Khomeini 12, 25–7, 31n36

Baghdad Pact 23, 30n32
Bakker, E. 34, 37, 41–2, 48, 50, 61
Bandung Conference 24
Bangladesh 26
Belgium 97n4
Bermingham, A. 88, 227
Beutel, A.J. 62–3, 76
Bjelopera, J. 41–2, 89
black swans 35, 38–9, 43; *see also* gray swans, outliers
Bolt, N. 86
bombings 28, 29n9, 201; Air India 167–8; attacks against US targets 35; Boston Marathon 187–90, 203, **206–7**; London Underground 110; Madrid train 110; selected sites 40

Borgatti, S.P. 51, 66, 68, 78, 221
Bossler, A.M. 129, 131, 135
Boston Police 187, 190
Bouchard, M. 1–3, 5, 7n1, 54, 65, 221–2, 225, 227
Bouhana, N. 92, 98n9
Bowman-Grieve, L. 85, 87, 109, 227–8
Brachman, J.M. 85, 107, 109
Brenner, S.W. 128, 133, 146–7
Brewer, M.B. 130
Brewer, R. 3
Briggs, R. 87, 89
Britain (Great Britain) 11, 13; Arab Bureau 15; Baghdad Pact 30n32; Muslim subjects 14; Prevent and Channel programs 37; *see also* British, United Kingdom
British 22–3; anti-Soviet organizations 23; authorities 14–15; Broadcasting Corporation (BBC) 61, 66–7, 70; colonialism 20; colonial territories 29n8; domination 17; House of Commons 37; IRA struggle 29n9; leaders 29n7; Middle East policy 16; Military Mission 20; operatives 13; reports 21; rule 18–19
Brodeur, J.-P. 163–4
Bronner, G. 93–4
Brooks, B.E. 196
Brooks, R. 61–2, 196
Burris, V. 54, 86, 227–8

Caiani, M. 86
Cairo Embassy to African Department 30n17
Campana, C. 83, 86
Canada–United States Beyond the Border agreement 185, 192
Canada–United States Cross-Border Crime Forum 185
Canadian: Access to Social Media Information (CATSMI) Project 180; Association of Chiefs of Police 176; O'Connor Commission 171n4, 183; Press 186; Security Intelligence Service 40, 158, 162–4, 167, 179
Carley, K. 49, 51–2, 55–6, 65, 158
Central Treaty Organization (CENTO) 30n32
Chen, H. 54–5, 86, 88, 156, 227
Chen, W. 51, 54–5
children 25, 37, 73, 201, 209; custody case 170n1; extremists target 108–9; Hammami's 67–8; of immigrants 35–6, 44n1; men without 21; pornography online networks 2, 55, 117; teaching 118
CIA (Central Intelligence Agency) 19–20, 22–5, 27, 30n16, 31n33, 31n39–40, 131, 161, 163
Citron, D.K. 190–1
colonialism 11; European 27; French 20
Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar 168–9, 171n4
Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182 168
Communications Security Establishment Canada (CSEC) 180; assistance requested 191; collaboration 182; collecting 192n4; mandate 162
communism 19; anti-communism 24; struggle against 25
communist 17; anti-communist 23; incursions 31
Conway, M. 53–4, 57, 82, 84–8, 106, 109, 223, 227–8
Coolsaet, R. 91–2
Coppock, V. 36–7
Correll, S.P. 130, 132, 141
Cottee, S. 42
counterintelligence 27; agencies 227; related content 167
counter-terrorism 49, 55, 163–4, 182, 209; agencies 6; bureaucracies 157; computation framework 197–8, 213; databases 190; Global Forum 178; investigations 181; measures 57; National Counterterrorism Center 168; operations 225; orthodoxy 156; preventive models 177; program 196; scholars 165; services 162
counter-terrorism policies 5–6, 57, 91; Canadian 175–6, 178, 218; United States 188
counter-terrorism strategy 56, 175, 186, 196; Canadian 4, 6, 177–8, 184
crime 2, *134*, *138*, *142*, *144*, 146, 177, 183, 198; Cross-Border Crime Forum 185; fighting 192; involvement 48, 128; organized 164; preventing 191; war 30n19
criminologists 48, 92
CT (counter-terrorism) strategy 177–80
cyber 2; actions 146; content 87, 89; deviance 129–30, 132; environment 133; dynamics 86; operations 162; protest 132; predictors of cyberactivism 129; warfare 131
cyberattacks 39, 128–30, 132, 135, 146–7;

interest in 223; politically motivated 131; predictors 141; willingness to engage in 129–30, 132, 135, 146–7, 223; world 137
cybercrime 130–1, 135, 137, 146; cybercrime-only model 140; cybercriminals 6; variables *134*, 141
cyberspace 90, 97n2, 129; attacks 133, 146; dynamics 83; leverage 82, 85; political extremists 86–7, 89, 91; radicalization patterns 88; terrorist group presence 84
cyberterror 141; cyberterrorism 6, 97n6, 156, 223; cyberterrorist attacks 6
cyberwarriors 6, 129, 146, 223; Chinese military 131; civilian 128, 141
cygnets 43; gray 35, 39–41, 44; tri-cultural 42; *see also* black swans, gray swans

Dagne, T. 61, 64, 66, 70, 75
Dalton, R. 131, 137
Dark Web project 54–5
Dawisha, A. 15, 17–18, 27, 29n7
Denning, D.E. 57, 97n6, 128–9, 141, 146
Ducol, B. 2, 6, 49, 54, 83, 86, 90, 222, 228
Dupont, B. 3–4, 6, 163–4, 189, 224–5

Earl, J. 131, 146
Earth First! (EF) 114, 117, *118*, 119, *120*, **121**, 122–3, *124–5*
Edwards, C. 84, 87–8, 98n8
Egerton, F. 86
Egypt 14–15, 17–19, 29n4, 30n31; 1967 war 24; border defense 23; corruption and poverty 27; former-Nazi advisors 20, 30n19; Hammani 64, 66–8, 70, 72–3, **74**, 76, **77**; institutions 22; Israeli raids 23; Naguib 22; US Air Force base 31n40
Egyptian 12, 18, 64; dictator 22–4; friend 73; government 22; military headquarters 30n31; Muslim Brotherhood 25; officer corps 22; Para-Military Forces 21, 30n23, 30n26, 30n28; soldiers 21, 30n20, 30n31; strongman 19, 23; teacher 17
Egyptians 22–3, 30n18
Everton, S.F. 49, 51, 56, 65, 78, 221

FBI (Federal Bureau of Investigation) 31n36, 61, 64, 66, 156, 161–3, 167, 185, 187, 190
Federal Court (Canada) 182, 191
female 137, 201
First World War 12–16, 29n4, 31n40; post-First World War mandate system 20
Fishbein, M.J. 133
Five Eyes 181, 191–2
Foreign Intelligence Surveillance Act (FISA) 163
foreign signals intelligence (SIGINT) 162, 180, 191; partnerships 178
former Soviet Muslims 24, 31n33; organizations 25
Forsyth, D. 199, **200**
France 11, 29n12, 97n4, 169
Freeman, L.C. 68
Freeze, C. 181–2, 191
French 13; Anglo-French invasion 24; Anglo-French Suez Canal Company 17; anti-terrorist unit 26; colonialism 20; jihadisphere 227; protectorate 15

Gartenstein-Ross, D. 41–2, 61–2, 76, 87
Gawande, A. 187
GENIUS system 197, 199–200, **201**, 202, 207, 212–13, **214**, 215; framework 210; simulations 203
Germany 20, 181; displaced person camps 25; imperial 14
Gerolymatos, A. 5, 28n1, 220–1, 226
Gershon, R.R. 209
Global Salafi Jihad 51–2
Government Accountability Office 160
Government of Canada 178, 180, 184–7, 196; Listed Terrorist Entities 114; Securing an Open Society 176
Government of Canada CSIS 180; Department of Justice 187; Department of Public Safety 178, 184; RCMP 185
gray swans 38–9; *see also* outliers

hacking *134*, *138*, *142*, *144*
Hacking, I. 38
Hagen, G. 14, 29n4
Hamas 28, 85, 108
Hammami, O. 3, 5, 61, 63–70, *71*, **76**, 79n1; network 66, 68–9, 71–3, **74–5**, **77**, 78; network density **76**; pre-jihad network 69, 72, **73**; radicalization 66, 78, 222; religious influences 79n3; trajectory 63, 65, 67–8, 72
Hankey, Lord 22; to Salisbury 21, 30n21
Hanyu, K. 198
Harris, C.P. 17–18
Hegghammer, T. 50, 61
Helfstein, S. 3, 53, 78, 221

Hezbollah 28, 85
Higgins, G.E. 130, 132–3, 137
Hinduja, S. 130–2, 135
Hoffman, B. 56, 155
Holt, T.J. 6, 128–30, 132, 135, 137, 141, 146–7, 223–4
holy war 11, 14, 19, 28
homegrown extremism 110–12; jihadists 39; jihadi terrorist plot 84; violent extremists 61
homegrown terrorism 51, 61, 64–5; terrorist groups 53; terrorists 1, 5, 34, 37, 42, 44, 61–6, 70, 73, 76–8, 222
Homeland Security Institute 87
Horgan, J. 2–3, 36–8, 41, 43, 48, 62, 76, 91, 93, 111, 222
HQBTE Report 21–2, 30n23–4, 30n26–8
Huddy, L. 130–1
Huey, L. 5, 38, 78, 218, 221
human intelligence through infiltration (HUMINT) 180

imperialism 27; American 26–7; Western crusading 11
India 14, 26, 31n40; Air India bombing 167–8; British 29n8
Indian authorities 121, 124; Muslims 29n8
Indonesia Bandung Conference 24
Ingram, J. 130, 135
injustice 62, 124; global 37; historical 11, 20, 27; perceived 136
Innes, M. 37, 164
Integrated Border Enforcement Teams (IBETs) 178, 184–5
Integrated Cross-Border Maritime Law Enforcement Operations (Shiprider) 178, 185, 188, 192, 224; *see also* NxtGen
Integrated National Security Enforcement Teams (INSETs) 164, 184–5
Integrated Threat Assessment Centre (ITAC) 181–3
integration 4, 6, 178, 189; in Canada 175, 192; in Canadian counter-terrorism 176–7; in denial strategies 184; emergency management 186–8; Hammami 70; information sharing 187, 190; of institutions 224; to jihadi networks 77; lack of 63; national security policing 185; networks 183; regulatory arbitrage 191; security intelligence 179–82; of technology 225
intelligence 159, 167, 177, 190–1; British 15–16; collection 183–4; community 24, 129, 225; cooperation 192; criminal 192n3; Egyptian 30n10; Five Eyes 181, 191; Foreign Intelligence Surveillance Act (FISA) 163; Foreign Intelligence Surveillance Court 161; foreign signals (SIGINT) 180; fusion centers 164, 166; gathering partnerships 192n1; German 20; global signals intelligence (SIGINT) 178; HUMINT 180; information 189; led 176–8, 182, 186, 188; materials 168; open-source (OSINT) tactics 180; operations 12; reports 114; security integration 179; sharing 169; swarm (SI) 199; TV shows 156; US agents 38; US community 162; *see also* intelligence agencies, intelligence organizations, intelligence services, Joint-Intelligence Group
intelligence agencies 146, 156, 166–7, 170, 176, 226; American 22; counter- 227; Pakistan 27, 31n39; security 177, 180; US 165, 169
intelligence organizations 30n16; Axis 13; Britain 15; Western 13
intelligence services Anglo-American 16; Britain 13; Canadian Security (CSIS) 40, 158, 162–4, 167, 179; West German 20
Internet 1–4, 53–5, 56–7; anonymity 128, communication 112–13, 155; intelligence 165, 226–7; propaganda 85; and radicalization 82–4, 86, 87, 88–90, 96–7, 220; as a recruiting tool 61, 63, 65, 66, 106–11, 122, 223; social networking 112, 222–3
Iran 12, 30n32; Iranian Revolution 25
Iraq 30n32, 31n41, 159, 163; capture of Al-Qaeda members 158; Soviet occupation 27; US occupation 28
Islam 18, 63, 65, 109, 219; conversion to 170n1, 218; converts to 37, 40, 64; Great Mosque 25–7, 31n34, 31n38; Hizbul 64, 75; jihad 112; legalistic interpretation 62; militant 15, 19; misappropriated 221; mosques 17, 40, 73; political 5, 12, 25; practice 64, 66–7, 72; radical 34–5, 37, 40; Salafi 72, 78; Shiite 27; socio-political ideologies 71, 76; state version 25; Sunni 27, 79n2; unity of 11, 13, 16–17; Wahhabi version 28
Islamic 14, 16–17, 64, 72, 170n1; Courts Union (ICU) 70; faith 18; Global Islamic Media Front (GIMF) 86; groups 113; homegrown terrorists 62;

ideologies 35, 77; jihad 27; messiah 31n35; militant organizations 26; precepts 19; radical movements 13; resistance 109; Salafi movement 79n2; State (IS) 15, 28, 219, 221; studies 67; University of Medina 25; world 11
Israel 12, 18, 20, 22–5, 28, 227; Israel–Palestine 122
Israeli 20; Arab–Israeli settlement 24; authorities 124; covert operations 30n31; paratroopers 26; raids 23; state 18
Israelis 12, 18, 28, 30n31, 109
Italy 11

Jackson, R. 37
Janbek, D. 83, 85, 87, 109, 112–13
Jawaharlal Nehru 24
Jenkins, B.M. 1–2, 34, 41, 61–2, 106
Jews 30n19; Jewish homeland 12, 15; Jewish settlers 18
jihad 11, 17, 19, 64, 66–7, 70–1, 156; in Afghanistan 27, 31n40; brother 79n3; calls for 108; context 113; declared 14–15; formal 110; Global Salafi 51–2; Internet 82; journey to 67–70, 74; leaderless 52–3, 112; ongoing 28; personal 61, 76–7, 222; pre-jihad **69**, 72, **73**
jihadi 70, *71*, 74, 77; brothers 5–6, 61, 66, 68–9, 73–4, 79n3, 222; global movement 85; homegrown terrorist plot 84; ideology 109–10; leaders 5–6, 64, 68, **69**, **73–5**, **77**, 79n3; materials 108; media 85–6; movement 107; recruitment 40, 111; websites 107, 109, 228
jihadisphere 227
jihadist 111; inspired movements 34; plots 35; terrorism 227; websites 226
jihadists 11–13, 18–19, 27–8, 110, 219; Al-Shabaab 66; arrested 40; Canadian 34–5; homegrown 39; would-be 111
Joffres, K. 51, 117
Johnson, I. 17–18, 25, 31n33
Joint-Intelligence Group (ISU-JIG) 181
Joint Terrorism Task Forces 163
Jordan, T. 128–9, 132

Kenya 72, 206–7; Westgate Shopping Mall attack 201, 206–7, **208**
Kilger, M. 128–30, 137, 141, 146–7
Kimmage, D. 85–6
King, M. 84, 87
King Farouk 19–20
King Faysal 25
Kirby, A. 110–11
Klausen, J. 54, 86
Kleinmann, S. 41–2, 89
Knoke, D. 50–1, 158–9
Kohlmann, E.F. 85–6
Koschade, S. 49, 65
Kosterman, R. 130, 135–6
Krebs, V. 4, 49, 65
Krueger, A.B. 37, 62
Kundnani, A. 37
Kunovich, R.M. 131

LaFree, G. 128, 146
Law Enforcement News 164
Lesser, I. 155
Lewis, J. 54, 57, 158
Lia, B. 16–17, 85
Liberation Tigers of Tamil Eelam (LTTE) 114, *118*, 119, *120*, **121**, 122–3, *124–5*
Libya 26, 219
Libyan 34
Lichtblau, E. 161–2
Loyal White Knights of the Ku Klux Klan (LWK) 114, *118*, 119, *120*, **121**, 122–3, *124–5*
Lynch, O. 36

McCauley, C. 1–2, 37, 91, 147, 219–20
MacCharles, T. 34, 218
McChrystal, S. 159
McCulloch, J. 37
Magouirk, J. 49, 52, 56
males 132; agents 201; Canadian 34; cybercrime-only 140; hackers 137; homegrown jihadists 39, 62; Muslim 34, 44; online protest activities 131; website target audience 113
Mandate C 180, 192n4
Markle Foundation Task Force 171
Martin, G. 128, 131, 133, 137, 146
Matza, D. 97n3, 130
Middle East 12–13, 18, 22–4, 31n36, 111; American policy 25; Baghdad Pact 30n32; British Mandate administrations 29n7; British policy 16; conservative governments 27; extremists and terrorists 19; protectorates 15, 20; radicals 29n12; terrorism 11, 29n9, 220–1; US government conduct 169
militants 11, 27, 31n38, 76; Islamic 16, 25; Middle East 16; Muslim 13, 18–19; Pakistani 26; radical 82–3; religious 18; well-armed 25

Mitchell, R.P. 11, 19
Mohamed, M. 64, 66–7
Molnar, A. 3–4, 6, 181, 188, 196, 224, 225
Monaghan, J. 180, 182
Morris, B. 18, 29n13
Morselli, C. 51, 53, 65–6, 71, 165
Moskalenko, S. 1–2, 91, 147, 219–20
Muslim 11–12, 14, 17–18, 186, 219; accusations of British perfidy 15; Brotherhood 11, 13, 16–19, 24, 28, 29n14, 221; CIA link 25, 31n33; club 64; first- and second-generation males 34; founded 29n10; groups 112; influential shaykhs 68, 73; intellectuals 23; paramilitary units 21; pure 66, 71, 78; scholars 74; Sunni communities 16; second- and third-generation men 36–7, 39–41, 44, 63; terrorism 27, 29n9; volunteers 22, 31n40; world 26
Muslims 5, 11–12, 16, 28, 37, 41, 111, 218; former Soviet 24, 31n33; global persecution 64, 72, 109; Great Mosque 25, 27, 31n34; Indian 29n8; languages 19; mass uprising 14; militant 18, 26; practicing 35; Shiite 29n3; Somali 72; Sunni 13, 15

Naftali, T. 20
Naguib, General M. 22
Nasser, G.A. 12, 16, 21; American relationship 20, 23–4; Arab nationalism 23, 27; assassination attempt 19, 29n15; desert concentration camps 30n18; intelligence network 30n19; revolution 18–19, 22; successor 31n40; undermined 25, 30n31
National Consortium for the Study of Terrorism and Responses to Terrorism (START) 187
National Security Investigations Sections (NSISs) units 184
nationalism 27, 130, *134*, 136, *139*, *143*, *145*, 146; Arab 13, 15–16, 22–3, 27; culmination of 12; in Egypt 18; Middle East 16; regional 17; secular 11, 16
Nazi 20, 25; ex-Nazis 20, 30n18–19; links 18; neo-Nazi escape organizations 20
Neuman, W.R. 89
Neumann, P.R. 2–3, 89, 91, 112, 226
Non-Aligned Movement 24
non-Muslim 11, 41; convert 35, 41; names 35, 40; terrorist groups 29n9
North Atlantic Treaty Organization (NATO) 30n32, 178
NxtGen (land-based extension of Shiprider) 192, 224; policing teams 185

O'Callaghan, D. 87, 228
Office of the Director of National Intelligence 190
Office of the Inspector General 167
Office of the Privacy Commissioner of Canada 179
oppression 11, 27, 62, 124, 221
O'Toole, L.J. 190
outliers 5, 35, 41, 44, 44n2, 221

Pakistan 30n32; Inter-Service Intelligence agency 27, 31n39; militant Islamic organizations 26; weapons shipped by US 31
Pakistani 26, 37; embassy staff killed 31n37
Palestine 15, 122; Arab revolt 17–18; *see also* Popular Front for the Liberation of Palestine
Palestinian 124; struggle 18; suicide bomber networks 52; victory 23
Palestinians 17–18, 28, 29n12, 122, 221
Park, A.J. 4, 7, 197–8, 201, **204**, **210**, **214**, 215
Passy, F. 94
patriotism 130, *134*, 135, *138*, *142*, *144*, 146; *see also* nationalism
Pedahzur, A. 49–50
Perera, D. 190
Perliger, A. 49–50, 52
Perry, R.W. 197–8, 213
persecution 11, 122; of Muslims 64, 72
Peters, R. 14
Pettigrew, T.F. 130–1
Pipes, D. 12
Piquero, A.R. 48, 133
police **209**; agencies 170; anti-terrorist officials 84, 97n4; Boston 187, 190; British 29n9; chiefs 164, 176; databases 167, 183; forces 156, 179; institution 159; local 163–4, 184; municipal forces 166, 181; New York 35, 160; officers 201–3, 213, 215; organizations 162–3; Pakistani 26; reports 185–6; Shiprider teams 188; Vancouver MLU 188, 192; *see also* Royal Canadian Mounted Police (RCMP), Secure Police Reporting and Occurrence System
Popular Front for the Liberation of Palestine (PFLP) 29n12, 114, *118*, 119, *120*, **121**, 122–3, *124–5*, 223

Porter, L.E. 37, 43
post 9/11 163; American policy 12; extremists 85; policies 177–8, 184; security discourse 189; terrorist networks 53; world 106, 160, 163
Post, J.M. 37, 131
postcolonial 12; Islam 11; world of the Middle East 19
Poulsen, K. 130, 141
Precht, T. 62, 87
Privacy International 181, 191
Privy Council Office, Government of Canada 176
Public Safety Canada 7n1, 114, 126n1, 179
Putnam, R.D. 128, 131, 146

Qin, J. 54–5
Qutb, S. 19, 29n14

Raab, J. 156, 169
radical organizations 11, 29n9; secular 12
radicalization 3, 6, 41–2, 44, 62–3, 82–4, 89–91, 97, 111–12, 179, 189, 220, 222; counter-radicalization initiatives 165; domestic 35–6, 43; homegrown terrorism 65, 76; individuals 1, 50; Internet 87–9, 107, 218, 226; literature 147; monitoring 178, 180; multidimensional approach 93; online 88, 106; self- 110; precursors to 63; prevention 37, 191, 192n2; progression to violence 62, 64, 74; recruitment 68, 70; research on 4–5; trajectory 61, 77–8, 79n1; understanding 92; violent 1–2, 49; of Westerners 34, 36
radicalization process 1, 5–6, 40, 43–4, 49, 53, 57, 61–3, 66, 68, 70, 72, 76–8, 82, 84, 87–8, 90, 92–5, 112, 147, 220; fostering 84, 89; Hammami's 78, 79n3; personal 2, 222
Ramsay, G. 83, 85–6
Reid, E. 35, 54, 86
Revolutionary Armed Forces of Colombia (FARC) 114, *118*, 119, *120*, **121**, 122–3, *124–5*, 223
Rhodes, R. 159
Richards, A. 36, 91
Roberts, N. 51, 56
Rodriguez, J.A. 49, 65
Rothenberg, R. 52–3
Royal Canadian Mounted Police (RCMP) 89, 164, 168–9, 171n4, 180, 182–4, 186, 192n3, 218; ISU 181; joint investigation 40; NSCO program 179; officers 34, 185; rigid rules 192n4
Russia 11, 13, 15; Russian Revolution 15; *see also* Soviet Union
Ryan, J. 226

Sageman, M. 1–3, 42–3, 48–53, 56–7, 61–2, 64–5, 78, 87, 112, 220
Salafi 79n2; Global Jihad 51–2; Global Network 53; Islam 72; movement 79n2; Qur'an teacher 64, 71, 77–8; scholar 71
Salafism 72
Schatz, R.T. 130–1
Schmid, A.P. 91, 129, 196
Schussman, A. 130–1, 146
Second World War 13, 16, 18–19, 24, 30n16, 31n40; post-Second World War period 11
Secure Police Reporting and Occurrence System (SPROS) database 182–3, 192n3
Sedgwick, M. 91
Seib, P. 83, 85, 109, 112–13
Shaheed Kalsa (SK) 114, *118*, 119, *120*, **121**, 122–3, *124–5*
Sheptycki, J. 167
Shia 25, 28
Shiite Baghdad government 28; Islam 27; Muslims 29n3
Sidanius, J. 136
Silber, M.D. 34–5, 37, 40–1, 87, 111
Silke, A. 86
Simon, J.D. 111
Simon Fraser University 7n1, 215
Situational Action Theory (SAT) 83, 90, **92**, 93, 98n9
Skinner, W.F. 129–32, 135, 137, 146
Smith, J.E. 24, 228n2
social networks 3, 49–50, 53, 62–3, 78, 96–7, 109–10, 155–6, 166–7, 220, 222, 225–6; social network analysis 43, 50, 51–2, 55, 61, 64–77, 88, 158
Soriano, M.R.T. 3, 226–7; *see also* Torres-Soriano
South American citizens 162
Southeast Asia Treaty Organization 30n32
Southers, E. 61–2, 65, 78
Soviet Union 13, 23–4, 30n16; British anti-Soviet organizations 23; defeat 12; financial support 24; former Soviet Muslims 24–5, 31n33; invasion of Afghanistan 26–7; prisoners of war 25; strategists 19
Spalek, B. 165

Sri Lanka 122, 124; *see also* Liberation Tigers of Tamil Eelam, Tamils
Statistics Canada 186
Stenersen, A. 85, 110
Stepanova, E. 129, 131–2, 147
Stroink, M.L. 36, 39
suicide 16, 27, 187; attacks 11, 112; bombers 28, 38, 52; squads 21; terrorists 109
suicide bombers 28, 38; Palestinian 52
Sykes, G.M. 130
Sykes–Picot Agreement 15, 20, 29n5
Syria 28, 63, 67, 72, 170n1, 183, 192, 219; Syrian family 63, 70, 72

Taleb, N.N. 35, 38–9
Tamils 122, 124; Liberation Tigers of Tamil Eelam (LTTE) 114, 119, **121**, *125*
Taylor, D.M. 84, 87
Taylor, M. 43, 91
Taylor, P. 128–9, 132, 146
Taylor, R. 164
terrorism homegrown 51, 61, 65
Terrorist Identities Datamart Environment (TIDE) 168
TE-SAT 82
Tessler, M. 36–7
Thompson, R.L. 213
Thompson Rivers University 215
Tilly, C. 97n1, 155, 166
Time 31n38
Torres-Soriano, M.R. 85–6, 226
Transportation Security Administration 168
Trofimov, Y. 26, 31n36
Tsang, H.H. 4, 7, 197
Tsfati, Y. 86, 107–8
Tsvetovat, M. 52, 56
Turkey 11, 26, 30n32
Turkish 13; Republic 16
Tyler, P. 23

United Kingdom (UK) 37–8, 97n4, 164, 181, 196
United States (US) 11–13, 16, 26–8, 37, 40–1, 70, 175, 177, 190; 9/11 terror attacks 128; administration 19, 25; air force 31n40; anti-terrorist fight 160; Army 159, 163, 188; Canada–United States Beyond the Border agreement 185, 192; counter-terrorism approach 196; cyberattacks 131, 147; Department of Defense 24; Department of Justice 162, 167; Department of State 24; Department of the Treasury 66, 79n4; Executive Order 79; Five Eyes 181; government 31n39, 170n1; homegrown terrorist Hammami 61, 63–4, 66, **69**, **73**, 75, **77**; Joint Terrorism Task Forces 163; links with Egypt 20, 22–3; nationalism 146; online political action *138–9*, 141, *142–5*; Patriot Act 161, 169; political action study 129, 132, *134*, 137; radicalized Muslims 41; targets 35; terrorist attacks 36, 186–7
United States (US) intelligence 162, 165, 167; budget 161; information sharing protocols 183; security 38, 169;
University of British Columbia 7n1
University of Waterloo 7n1, 215

Vancouver 2010 Olympics 181, 185, 188
Van Laer, J. 128, 130, 132
Verba, S. 131, 137
Vollhardt, J.K. 130–1, 136
Von Behr, I. 90, 98n8

Washington Post 159, 162
Weimann, G. 54, 82, 84–7, 106–11, 156
Westlake, B. 55, 117
Whelan, C. 3–4, 225
Wikström, P.-O.H. 92, 98n9
Wiktorowicz, Q. 63, 76
Williams, M.M. 209
Williams, P.L. 35
Wilner, A. 36, 42–3, 61–3, 76
Wilson, P.W. 26, 31n38
women 19, 25, 28; website materials targeting 113; wives 64, 67–8, 70, *71*, 73, 75, 77, 170n1
Woo, H. 129, 146
Woods, A. 184, 218–19

Xu, J. 39, 55, 65, 156

young men 19, 34–5, 65, 72

Zanini, M. 54, 56
Zelin, A.Y. 86
Zellner, A. 41
Zhou, Y. 54–5, 227
Zhou Enlai 24